Remotely Piloted Aircraft: The Challenges of Force Integration

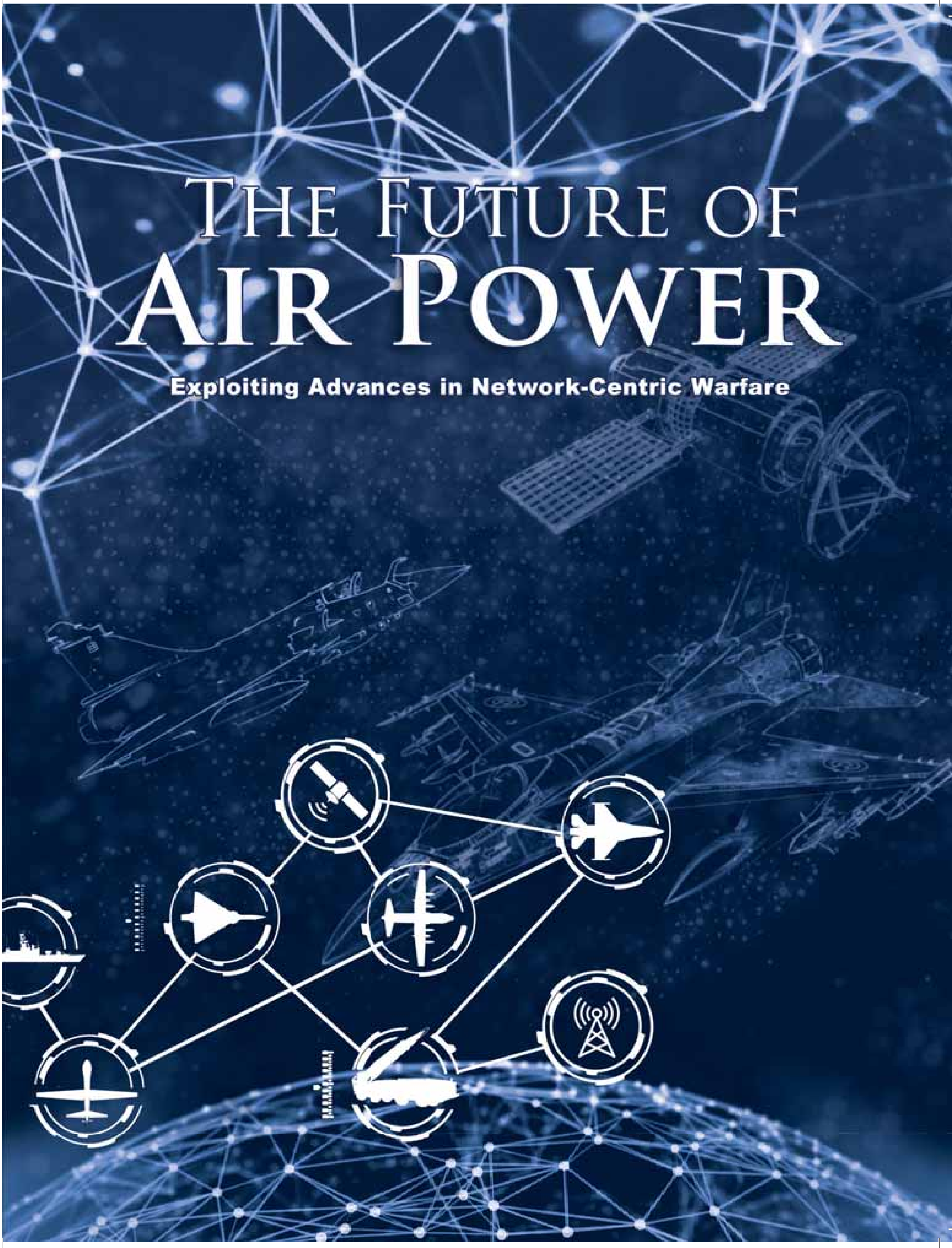
Schaub Jr, Gary John

Published in:
The Future of Air Power

Publication date:
2017

Document version
Publisher's PDF, also known as Version of record

Citation for published version (APA):
Schaub Jr, G. J. (2017). Remotely Piloted Aircraft: The Challenges of Force Integration. In *The Future of Air Power : Exploiting Advances in Network-Centric Warfare* (pp. 47-52). Inegma. Institute for Near East and Gulf Military Analysis.


THE FUTURE OF
AIR POWER
Exploiting Advances in Network-Centric Warfare

Institute for Near East and Gulf Military Analysis

Printed in the United Arab Emirates

Contents

Preface 3

Developing Fifth Generation Air Power Capabilities – Key Imperatives and Challenges for Future Force Planning 4
Dr Andrew Davies

Interoperability Challenges between 4th and 5th Generation Aircraft 10
Justin Bronk

Air Force Challenges Today, Impact on Force Planning Tomorrow – A Look at the United States 16
Vago Muridian

Strategic Mobility and Rapid Response – Core Enabling Capabilities for Coalition Air Operations 22
Dr. Christian Mölling and Torben Schütz

C4I and the Challenges of a Coalition Environment 28
Douglas Barrie

A UAE Perspective on Transformation to Network Centric Operations (NCO) 32
Major General (Ret.) Khalid Abdullah Al Bu Ainnain

ISR Challenges against Asymmetric Threats and Plugging Gaps in the Sensor-Shooter Network 40
David A. Deptula, Lieutenant General, USAF (Ret.)

Remotely Piloted Aircraft: The Challenges of Force Integration 45
Dr. Gary Schaub, Jr.

Trends in Ballistic and Cruise Missile Technology and its Impact on Counterforce Planning – A South Korean Perspective 51
Sung Kurl Kim Ph.D.,

The Future of Integrated Air Power and Missile Defense in the Arabian Gulf 57
Thomas Karako and Wes Rumbaugh

Airpower in Counter-Terrorist Operations: Balancing Objectives and Risks 64
Adam R. Grissom Ph.D. and Karl P. Mueller Ph.D.

Exploiting Network-Centric Operations (NCO) for Information Superiority 68
Sabahat Khan

The Future of the 'Air Force' – An Integrated Part of a Broader Defense and Security Eco-System 74
Stephan De Spiegeleire

Photo: Al Jundi Journal

Preface

Fifth-generation capabilities and Air Force transformation towards network-centric operations (NCO) offer a new horizon of possibilities. Unprecedented levels of situational awareness promise compressed decision cycle times and more precise effects in operations for the Air Force. With these developments however new dependencies will arise, for example, on space-based platforms, remotely piloted vehicles (RPAs), and the effective exploitation of information systems, information-sharing, and automated processes – generating new risks together with new opportunities. The air, space, and cyber domains will become more amalgamated with the land and sea domains as the battlespace becomes more contagious and continuous. Networked capabilities will enable the Air Force to interoperate in unprecedented ways for Combined, Joint and Coalition operations. NCO will also make the Air Force more dynamic in its ability to adapt to changing needs and in its ability to self-synchronize to achieve the Commander's intent. Yet the challenges of force transformation towards NCO and truly fifth-generation capabilities are often rooted in human factors and rigid institutional approaches or cultures than by technological limitations. This publication brings together the latest perspectives from a collection of international experts to provide insights into harnessing NCO through technology and related concepts to impart a set of visions on the future of air power.

Developing Fifth Generation Air Power Capabilities – Key Imperatives and Challenges for Future Force Planning

Dr Andrew Davies
Director, *Defence and Strategy Program, Australian Strategic Policy Institute*

Air Superiority and Fifth Generation Capabilities

Discussions of the implications of fifth generation technologies for western air power are usually couched in terms of the benefits of stealth, advanced situational awareness and other technological advantages. Doubtless many of the other papers in this volume address those issues. This paper will take a different approach, because I think that there is too much focus on the benefit of technologies. A focus on the highest level of capability risks losing sight of the main reason for nations to expend resources on air power – helping to win wars when it is critical to do so.

There is no doubt that, all other things being equal, it is better to enter air combat with the more technologically advanced aircraft, and with the support systems in place to make best use of that technology. In conflicts over the past thirty years, western air forces have been able to exploit their technological advantage and bring air power to bear decisively and dramatically. But those conflicts have been against non-peer powers with limited or dated air defence capabilities.

There has been a profound mismatch between the defensive capabilities of countries such as Iraq, Serbia, Libya, Yemen and Syria and the air forces of NATO, the United States and other nations (including Australia), that are equipped with advanced western technology. The results have been as expected – any air threats have been


Photo: Lockheed Martin

quickly neutralized, and coalition forces have been able to conduct strikes at will. Combat losses and casualties to the air forces involved have been very low.

Because of those dramatic examples of air supremacy, there has been a tendency among western air forces to plan their future forces around the highest available levels of technology – what I call 'silver bullet' capability solutions. But there is a risk that doctrine and force structures derived from experience of 'wars of discretion' against significantly weaker forces will not be appropriate for more challenging future contingencies against more sophisticated adversaries.

The costs of capability

There is no doubt that the unit cost of combat aircraft has increased substantially over time, as is shown by a wealth of data dating back a century. The cost growth of combat aircraft (in fact of all military platforms) has far exceeded inflation.[1] Fighter aircraft have increased in price at a rate far above inflation since they first appeared around the outbreak of the First World War.

Of course, unit capability has also increased dramatically. But that capability comes at a cost to the numbers of aircraft that can be afforded. The United States Air Force (USAF) currently possesses the finest air-to-air platform in the world today, in the form of the F-22 Raptor – the first fifth generation aircraft to be fielded. But it was also prodigiously expensive to produce. As the unit cost of the aircraft pushed towards the USD$200 million mark, production numbers fell dramatically. The USAF originally wanted 648 Raptors. It eventually got 187 operational aircraft.[2] It is a similar story when we look at bombers. The USAF wanted 132 examples of the B-2 Spirit, and eventually got just 21.[3]

A reduction in numbers due to the cost is not the only impact of demanding increasingly sophisticated aircraft; development programs are taking longer than ever before. The early stages of development of the F-35 Lightning II began more than two decades ago, and the aircraft is only just entering operational service today. To make matters worse, the early aircraft will lack many of the capabilities envisaged for the type

Photo: Eurofighter Typhoon

at design. By the time the F- 35 is flying with most of its designed capabilities, it will be more than a quarter of a century after the preliminary studies commenced. And, as was the case for the programs mentioned above, substantial increases in the unit price compared to the original estimate has already impacted on planned production numbers. Authorized purchases by the three American services have already been reduced from 2,866 to 2,457.[4] It remains to be seen how many will eventually be produced – but it is clear that the future inventory of American strike fighters will be smaller than the current force.

> The high cost of recapitalization and the lack of available replacements mean that it is not unusual for combat aircraft to remain in service for several decades

The net result of increasing prices and longer development programs is that aircraft are kept in service longer. The high cost of recapitalization and the lack of available replacements mean that it is not unusual for combat aircraft to remain in service for several decades. To quantify that trend, the average age of strike fighters in the USAF inventory in 1980 was ten years. Today it is over 20 years.[5] The longer an aircraft remains in service, the more likely it is that an adversary will be able to field a competitor, to develop countermeasures to that aircraft's systems, or both. The USAF's F-15s and F-16s were probably the finest combat aircraft in the world in the 1980s and 90s. They are still formidable today, but newly developed platforms in China and Russia drastically narrow the capability gap. Even the F-22 needs a technology refresh to keep it at the leading edge of capability.[6]

Numbers matter

The identified trends of rising costs and smaller numbers would be acceptable if they were offset by the high capability provided by 'silver bullet' platforms. In fact, by concentrating on ever-more-sophisticated (and thus ever-more-expensive) aircraft, and thus reducing numbers, there is a real possibility that the total air power that could be brought to bear in a high-end scenario by the USAF and other western forces has gone down.

Consider the outcomes of a 2009 RAND Corporation study on a hypothetical conflict between the Chinese air force (PLAAF) and the combined forces of the United States and Taiwan.[7] The study scenario involves a pre-emptive Chinese attack on Taiwanese and U.S. bases and ground-based air defence assets to blunt their ability to thwart a Chinese invasion of Taiwan. In this scenario an air war for supremacy over the Taiwan Strait ensues.

RAND made some analytic assumptions about the relative capability of American and Chinese aircraft. In one-on-one engagements, they assumed that the exchange ratios would be heavily in favor of U.S. forces (see Table 1 below).

Table 1. 2009 RAND Corporation study assessment of relative combat effectiveness of American and Chinese aircraft over the Taiwan Strait.

Aircraft	Exchange ratio
F-15	4.5 : 1
F-22	27 : 1
F/A-18	2.6 : 1

Calculating the numbers in the table depends on knowledge of sensor and weapons effectiveness, radar cross sections at various wavelengths, missile kill probabilities, and the tactics employed by the combatants. But it turns out that the exchange ratios are surprisingly unimportant in the big picture. Despite the huge advantage to American aircraft in individual battles implied by the figures in Table 1, the PLAAF campaign is successful in many of the simulations.

Photo: Dassault Rafale

In this scenario both sides suffer significant losses – especially the Chinese, as would be expected from those unfavorable exchange rates. But in wars in which core national interests are engaged, avoiding casualties matters less than winning. Silver bullets are wonderful when losses are unacceptable and the opposition is weak, but other factors come into play when the stakes are higher.

A similar RAND study conducted in 2000 provides an interesting counterpoint.[8] In the earlier study the Chinese were almost always defeated. So in the space of nine years the Chinese air forces (as modelled by RAND) managed to close the gap – at least in the specific case of an air war over the Taiwan Strait. The way in which they did so did not depend on 'silver bullet' technology. It is true that the average quality of their aircraft had improved due to the modernisation program that all PLA forces have been undergoing. But, as Table 1 shows, there was still quite a capability gap between Chinese and USAF types.

The key reason was the ability to be able to generate enough sorties to allow a quantitative difference in combatant numbers to compensate for the qualitative advantage enjoyed by the Americans. Table 2 below tells the other – and ultimately decisive – side of the story.

Table 2. 2009 RAND Corporation study estimation of combat sortie generation of American/Taiwanese and Chinese forces over the Taiwan Strait.

Country	Mission	Type(s)	Sorties
China	Air base attack	Su-30, J-10	337
	Other attack	J-8	74
	Escort	J-8	97
	Sweep	Su-27/F-11, J-8	290
		Red total	798
Taiwan	Air defence	Various	100
US	Air defence	F-22	20
		F/A-18 E/F	96
		Blue total	216

We can understand the results of the 2009 study in terms of the total combat effectiveness of the two sides. The required tool is the Lanchester law of aimed fire – a mathematical relationship first formulated to describe air combat in the First World War. Lanchester's 'square law' tells us that it is the square of the number of aircraft in the fight that characterises force level effectiveness.[9] Given equally capable platforms, if blue force has twice as many aircraft as red, then the overall blue combat effectiveness is four times greater.

That observation is all we need to understand the 2009 RAND study results. The advantage the Chinese enjoy of being able to use land bases to generate multiple sorties per day from a multitude of nearby bases overwhelms the technologically superior U.S. forces. The Americans must operate either from land bases well-removed from the battlespace or from carrier decks, while the PLAAF has 27 air bases within 500 nm of the Taiwan Strait. The US has just one at Kadena, Okinawa. That disparity makes the PLA's airfield denial strategy much easier. And the air threat to the carriers means that they must be kept at a safe distance.

Because of the distances involved and the relatively small number of American sorties that can be generated, the phenomenal advantage in individual combat provided by the F-22 makes little difference to the outcome. The bulk of American sorties are flown by Super Hornets flying off carriers. The average of exchange ratios weighted by sorties is still 6.8:1 in favor of the Americans, but that cannot compensate for the numerical advantage of the number of Chinese sweep and escort sorties. The ratio of Chinese to American sorties is 387:116 (counting only American sorties because in the RAND analysis the Taiwanese air force very quickly loses the ability to operate from its bases because of early Chinese strikes). Applying Lanchester's rule, the square of the sortie ratio is a little over 11:1 in favour of the Chinese side, enough to give the Chinese an advantage, provided that their aircraft are at least competitive with the Americans.

Conclusion

Modern western air forces are evolving into relatively small forces of extremely capable platforms. Their advanced fourth generation and fifth generation types have sensors, weapons and networking that allow them to fight without loss (or with very few losses) in a the circumstances that have prevailed over the past few decades.

But if current trends continue, future types will take longer to develop and they will cost more at the end of the development process. The net result – especially given the sluggish performance of many western economies in the decade after the global financial crisis of 2008 – will be a further reduction in the size of fleets.

Even small fleets of more capable aircraft might suffice for operations of the type the U.S. and its coalition partners have carried out in recent years. But the analysis discussed in this paper suggests that that model might be found wanting if there is a conflict with a near peer competitor. Numbers really do matter if losses are acceptable. A larger number of less sophisticated aircraft can defeat an adversary with better ones. The RAND analysis does not discuss a lengthy war in which attrition matters, but a drawn out conflict would also tend to favor the side with the greatest numbers, which would be best able to sustain losses.

The conclusion I draw from these considerations is that future development programs should concentrate more on delivering a credible capability faster and at lower cost as opposed to slowly delivering the best possible capability at great expense. Cost needs to be a greater factor when making decisions between desired levels of capability. Otherwise, there is a risk of facing an existential crisis with a force that is exquisitely capable but too small to prevail when it counts.

References

1- There are many good charts in Norman R. *Augustine, Augustine's Laws – an irreverent guide to traps, puzzles and quandaries of the defence business and other complex undertakings.* American Institute of Aeronautics and Astronautics, New York, 1983.

2- For a summary of F-22 development and procurement, see *F-22 Raptor, Federation of American Scientists. Available at* https://fas.org/man/dod-101/sys/ac/f-22.htm (Accessed 30 June 2017)

3- B-2 Spirit. , Federation of American Scientists. Available at https://fas.org/nuke/guide/usa/bomber/b-2.htm (Accessed 30 June 2017)

4- As recorded in successive editions of the Government Accountability Office (Washington) Assessments of Selected Weapon Programs annual report. The most recent edition is available at http://www.gao.gov/assets/690/683838.pdf. (Accessed 30 June 2017) The F-35 program is on pages 165–166.

5- For a recent discussion of the ageing of the USAF fleet, see U.S. Military Power: air force, Heritage Foundation (Washington). Available at http://index.heritage.org/military/2015/chapter/us-power/us-air-force/ (Accessed 30 June 2017)

6- *See the 2017 Assessments of Selected Weapon Programs* cited above, pages 141–142, for a description of the upgrade program.

7- David A. Shlapak et al, *A Question of Balance: Political Context and Military Aspects of the China-Taiwan Dispute*, RAND Corporation, Santa Monica, 2009. Available at http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG888.pdf (Accessed 30 June 2017)

8- Shlapak, David A., David T. Orletsky, and Barry A. Wilson, *Dire Strait? Military Aspects of the China-Taiwan Confrontation and Options for U.S. Policy*, RAND Corporation, Santa Monica, available at http://www.rand.org/pubs/monograph_reports/MR1217/ (Accessed 30 June 2017)

9- For an introduction to Lanchester's laws, see the U.S. Naval Academy paper by Joyner, *An introduction to systems of DEs:Lanchester's equations for battle.* (undated) Available at https://www.usna.edu/Users/math/wdj/_files/documents/teach/sm212/DiffyQ/de-lanchesters-eqns.pdf *(Accessed 30 June 2017)*

The current paper is an expanded version of a blog post: Andrew Davies, *Geek of the week: Frederick Lanchester, and why quantity has a quality all of its own.* 20 September 2013. Available at https://www.aspistrategist.org.au/geek-of-the-week-frederick-lanchester-and-why-quantity-is-a-quality/ *(Accessed 30 June 2017)*

Andrew Davies has been with the Australian Strategic Policy (ASPI) Institute since 2006. He has written extensively on Australian defense capability and force structuring issues, including platform options for air and maritime combat, industry issues, and decision-making in the Australian Department of Defence. He has an ongoing interest in the future submarine and Joint Strike Fighter projects, and his work on both has made an important contribution to the public understanding of those projects in Australia and abroad. Before joining ASPI, Andrew was a post-doctoral fellow in physics at Melbourne University and the Australia National University. He then spent twelve years in the Australian Department of Defence in the areas of capability analysis and intelligence.

Andrew Davies

Interoperability Challenges between 4th and 5th Generation Aircraft

Justin Bronk
Research Fellow for Airpower and Technology, *RUSI*

Fourth- and Fifth-Generation Aircraft Connectivity

4th and 5th generation fighter aircraft constitute two blurred categories into which manufacturers and enthusiasts attempt to place or benchmark their chosen favoured types. However, for the sake of clarity, this analysis will treat these as referring to aircraft designed with differing combat philosophies in mind. 4th generation fighters will be thought of here as those designed with speed, aerodynamic agility, radar performance and missile loadout as foremost concerns. 5th generation fighters by comparison are considered to be those designed with the aim of minimising their detectable signatures to radar and IR sensors through airframe shaping and buried sensors, whilst maximising their own information advantage through low-probability of intercept radar scanning, advanced passive tracking capabilities and high-end sensor fusion. As might be expected when viewed in these terms, 4th and 5th generation fighter aircraft possess a host of different attributes, strengths and weaknesses which generate both challenges and opportunity when used together as part of modern complex air operations.

5th generation aircraft must make various aerodynamic and payload concessions in order to be shaped to minimise short-wave radar returns. They must carry their weapons in internal bays which seriously limits payload size, reduces space available for internal fuel and increases airframe

Photo: Lockheed Martin

weight and complexity. However, internal weapons carriage also grant a much more streamlined aerodynamic profile in combat configuration compared to 4th generation fighters. A major feature of the design philosophy and operational tactics built around remaining undetected wherever possible for as long as possible is that communications options for 5th generation fighters with legacy aircraft are limited and problematic. When an aircraft broadcasts on Link 16 or via a SatComm uplink, it gives off detectable electronic emissions which can give away its location to sophisticated opponents. Therefore, 5th generation aircraft such as the F-22 and F-35 were designed to communicate using low-probability of intercept (LPI) datalinks such as Chameleon and the Multifunction Advanced DataLink (MADL). These datalinks allow information to be shared in flight without compromising survivability but they cannot be picked up and deciphered by legacy 4th generation platforms without modifications and additional equipment. Therefore, the first and most important challenge standing in the way of regular interoperability between 4th and 5th generation fighters is finding a way for them to exchange data in flight without risking revealing the position of the 5th generation aircraft to enemy passive tracking sensors.

> 5th generation aircraft must make various aerodynamic and payload concessions in order to be shaped to minimise short-wave radar returns

Current Approaches to Interoperability

So far, two main approaches to this problem are being developed by the U.S. Air Force (USAF) and its allies. The first is to use an airborne gateway relay and datalink 'translation' capability mounted on another platform such as an EQ-4 Global Hawk or business jet derivative. This approach relies on having the relay platform positioned with a line of sight of the combat zone which requires high operating altitudes in order to maximise line of sight distances. It also requires a reasonable transit speed in order to move with a strike group; or knowledge of where engagements will take place in advance coupled with high endurance so as to be ready when needed. The primary relay and translation payload used by the USAF for this role is Northrop Grumman's Battlefield Airborne Communications Node (BACN). The advantages of this approach are a large number of simultaneous multi-waveform communications channels available to the whole force, including naval and land assets, and the capacity to extend the range across which 5th generation fighters can send and receive data, whilst translating their LPI datalinks into Link 16 for 4th generation colleagues. The disadvantages include the high cost of specialised large unmanned aerial vehicles (UAVs) with BACN nodes, the fact that they can be kinetically targeted by opponents more easily than fighters if they can get within missile range. This approach also adds to the mission planning and coordination burden due to the need to manage the relay aircraft in addition to combat jets and normal support enablers.

The second approach to solving the communications interoperability challenge is to add relay and translation pods to the payload carried by some 4th generation fighters in a mixed formation, such as Boeing's Talon HATE system. Talon HATE is a podded system which fits under the centreline of 4th generation F-15C Eagle fighter aircraft and allows them to communicate using LPI datalinks with the F-22 Raptor, as well as giving them secondary SatComm and air-ground relay capabilities. The benefits of this approach over a dedicated relay and translation node carried on a separate support airframe are that the 4th generation fighter can keep up with the other fighters in the strike package and can defend itself if attacked just as well as any other 4th generation fighter. However, it also reduces the payload weight that can be carried by the relay-node equipped fighters at the expense of potential missiles and fuel, and offers less potential bandwidth and sustained multi-user connectivity than a dedicated high-altitude relay system, especially if the carrying fighter is forced to manoeuvre aggressively.

> **5th generation fighters have** strengths and limitations which almost perfectly balance out the strengths and weaknesses of 4th generation air superiority aircraft

The benefits of allowing 4th and 5th generation fighters to communicate seamlessly without compromising the survivability of the latter are multifaceted and extremely potent. 5th generation fighters such as the F-22 and F-35 have strengths and limitations which almost perfectly balance out the strengths and weaknesses of 4th generation air superiority aircraft – especially modern examples such as the Eurofighter Typhoon and F-15SA. An F-22, for example, is exceptionally capable of detecting and avoiding detection by other fighter aircraft, but it is capped in terms of how many 'kills' it can achieve in each sortie by its internal missile and fuel limitations. By contrast, an F-15SA can carry up to sixteen air-to-air missiles as well as external fuel tanks to extend time on station and combat persistence, but is less capable of detecting and avoiding detection by hostile aircraft when in combat. Put together, in this scenario, the F-22 can make the F-15 much more survivable against advanced air (and ground) threats by relaying its own superb situational awareness picture back to the F-15

Photo: Eurofighter Typhoon

whilst the latter stays back from harm's way. At the same time, the F-15 or any other 4th generation fighter which is properly linked can provide the numerically limited 5th generation side of the force with a large number of missiles and usable fuel for manoeuvres. This paring of 'thugs and assassins' allows the 4th generation fighters to thin down opposing forces using volleys of missiles whilst the 5th generation fighters conserve their own fuel and missiles for either the last stages of an engagement or for any particularly dangerous threats.

The same principles hold for missions involving the suppression of complex integrated air defence systems (IADS). In order to remain stealthy and able to get relatively close to modern air defence threats without being detected, 5th generation fighters must rely on internally carried weapons only. However, even a 5th generation fighter can be detected by air defence radars from certain angles, ranges and at various frequencies. Therefore, whilst as a rule of thumb they can get closer to high threat systems than legacy aircraft, they still need to maintain as much distance from radar systems as possible – which makes attacks with the small air-to-ground munitions suitable for internal carriage on stealth fighters risky. By contrast, fourth generation fighters are capable of carrying large external payloads including long range cruise missiles with low radar cross section (RCS) such as Storm Shadow and JASSM-ER, as well as traditional anti-radiation missiles such as ALARM and AARGM. These standoff munitions allow 4th generation fighters to launch attacks against ground targets from outside the range of even the longest-ranged surface to air missile system currently in operation – the Russian S-400.

However, what the 4th generation fighters cannot do is provide these standoff munitions with the accurate, real-time targeting information that they need to hit small, mobile air defence radars and launchers from such distances. By integrating in a combined force with 5th generation fighters which can get close enough to enemy air defences to detect and track them in real time without high risk to themselves, 4th generation fighters can be supplied with the required targeting information to make standoff attacks on key nodes and open up a window for other assets. At the same time, this standoff attack capability allows the destruction of enemy air defence nodes without having to risk 5th generation fighters unnecessarily in free-fall or glide bomb attacks from their own internal payloads.

Tactical Interoperability between Fourth- and Fifth-Generation Aircraft

Beyond the mutually complementary strengths and weaknesses in terms of sensors, stealth characteristics and payload between 5th and 4th generation fighters, there are many more advanced tactical opportunities and challenges involved in their tactical interoperability. One of the most important challenges in terms of operationalising 4th-5th generation pairing comes from the simple fact that from most angles 5th generation fighters do not show up on fighter radars and that during combat they will minimise their signals emissions to avoid giving themselves away. This means that without proper mission planning, it can be very hard for friendly aircraft to keep track of where their 5th generation colleagues are. This can pose problems for weapon firing safety parameters, flight deconfliction and tactical decision making. This is difficult enough in air-to-air combat situations where fighter deconfliction and target prioritisation are the main issues, but is a much more complex when 4th and 5th generation fighters form part of a complex strike package alongside UAVs, electronic warfare assets, intelligence, surveillance, tracking and reconnaissance (ISTAR) aircraft and other components. In such cases, the inclusion of low-observable 5th generation aircraft can make mission timetables rigid and cumbersome if separation has to be maintained simply through pre-planned timelines and flightpaths. It also makes it fairly obvious to defending enemy forces where 5th generation aircraft are likely to be if there is a large incoming force showing up on radar with a strange 'empty gap' in the middle. Once again, a key requirement for dealing with these challenges is a translation and relay capability to allow 5th generation fighters to update friendly aircraft via LPI datalinks.

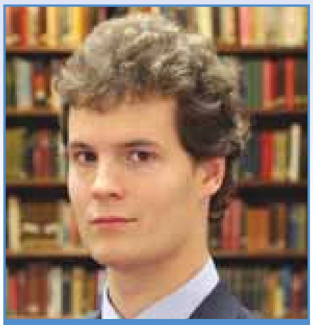
> **5th generation fighters do not show up on fighter radars and during combat they will minimise their signals emissions to avoid giving themselves away**

None of these are insurmountable challenges, but they do mean that for air forces with 5th generation assets working alongside legacy jets, mission planning and execution are significantly more complex and require a great deal of practice to perfect. However, as already outlined there are huge advantages to be gained in terms of the combat potential of both 4th and 5th generation types from true interoperability. Beyond the payload and fuel advantages of 4th generation fighters and the sensor and survivability advantages of 5th generation, their integration poses many challenges for opposing forces due to the difficulties of optimising forces to defeat both types at once. In order to detect and defeat 5th generation fighters, enemy aircraft and ground systems must concentrate their radar and other sensor resources on the occasional 'ghost' returns that might indicate their presence. However, this is much harder to do with 4th generation fighters also in the mix which are much more visible but still extremely dangerous especially when being fed situational awareness by their 5th generation brethren. In other words, opposing forces face a choice of either devoting less sensor and operator capacity towards trying to find 5th generation fighters by focussing on fighting the 4th generation threats which they can see, or at least partially ignoring 4th generation threats to try and detect the considerably illusive 5th generation fighters which they know are somewhere nearby and represent the most dangerous order of battle threat to them.

Conclusion

In either case, the survivability and mission effectiveness of the whole force is enhanced by using 4th and 5th generation assets together. Given the expense of 5th generation fighters and, therefore, the slow pace and quantity of procurement, this is the future of the Western way of air warfare for the foreseeable future. 4th and 5th generation fighters are already being used together but true interoperability across NATO and beyond will take time and investment to realise. The potential capability benefits nevertheless make such investment and effort essential.

Justin Bronk is a Research Fellow specialising in combat airpower and technology in the Military Sciences team at the Royal United Services Institute for Defense and Security Studies (RUSI) in London, United Kingdom. He is also Editor of the RUSI Defense Systems online journal. Justin has written on air power issues for the RUSI Journal, RUSI Defense Systems, RUSI Newsbrief, the Journal of Strategic Studies and the RAF Airpower Journal, as well as contributing regularly to the international media. He holds an MSc in the History of International Relations from the London School of Economics and Political Science, and a BA (Hons) in History from York University.



Justin Bronk

Photo: U.S. Air Force

Air Force Challenges Today, Impact on Force Planning Tomorrow – A Look at the United States

Vago Muradian
Editor, *Defense & Aerospace Report*

The Evolution of the U.S. Air Force

As air forces enter their second century, they are busier than ever performing a wider array of missions.

For the U.S. Air Force – which celebrated its 70th anniversary this year – the challenge is particularly acute. It the smallest it's been since 1947 as it makes a generational, institutional shift to address major power competition from Russia and China across air, space, strategic deterrence and cyber operations.

At the Cold War's end, the U.S. Air Force stood alone as the world's most capable air force with strategic and tactical nuclear weapons, overwhelming conventional strike, airlift, refueling, surveillance, space as well as nascent remotely piloted and cyber capabilities.

Since the 1991 Gulf War, a force shaped by the Cold War has spent 26 years in continuous combat air operations, the last 16 years of which have been the permissive airspace over Afghanistan, Iraq, Libya, Yemen, Somalia and Syria. Driven by insatiable post-9/11 intelligence demands, an ever-larger portion of a shrinking force has been devoted to operating and maintaining remotely piloted aircraft and analyzing and distributing the growing volume of intelligence generated by ever more sophisticated sensors.

Over the past 16 years, the U.S. Air Force focused on counterinsurgency and counterterror operations with strike, airborne and space reconnaissance, lift, communications, imagery and global positioning system (GPS) services. And it maintains two-thirds of nation's nuclear deterrent capability with more than 400 land-based intercontinental ballistic

Photo: Lockheed Martin

missiles and nuclear-equipped bombers, a force that operates and deters every day.

The ability of the U.S. to strike any target, anywhere with precision – first demonstrated during the 1991 Gulf War – has driven adversaries to invest in systems to undermine America's advantages and push U.S. and allied forces far from their borders and make operations over contested airspace increasingly costly.

As a result, the U.S. Air Force must prepare itself for a future of major power competition where it must credibly conduct operations in highly contested airspaces. It will also be a future where the U.S. Air Force may face loss rates unseen since the Vietnam War, during which it lost 2,251 aircraft.

Over the past 25 years, the most challenging air defense environment experienced were the skies over Serbia, where the current U.S. Air Force chief, General David Goldfein – then a Lieutenant Colonel – in 1999 became the last U.S. pilot shot down during operations against the country's armed forces when his F-16 was hit by an SA-3 surface-to-air missile. Goldfein was quickly rescued. In 2006, Major Troy Gilbert was the last U.S. Air Force pilot downed and killed by enemy ground fire over Iraq during a low-altitude strafing run.

Chinese, Russian, Iranian and North Korean investment in anti-access, area-denial (A2/AD) capabilities present the U.S. Air Force with a series of complex challenges aimed at blunting the deterrent power of the United States that for decades has counted on the ability to rapidly strike any target anywhere in the world with conventional airpower.

Countering Air Threats

The U.S. Air Force's deterrent has been a stabilizing influence, giving adversaries pause as they consider military operations against the United States, its allies or interests. Any action that undermines this deterrent capability could lead to greater global instability. Under budget constraints and facing rising costs for new equipment as well as manpower -- the service's most expensive commodity – the force personnel were cut to free resources for new systems to cope

with operational demands and emerging threats. Today, the U.S. Air Force has 318,000 active – plus 174,000 Air Guard and Reserve – airmen and about 5,400 aircraft. That's down from 535,000 active airmen alone in 1991 and 8,700 aircraft with another 2,500 Air Guard and Reserve planes.

But in many mission areas, as the U.S. Air Force has gotten smaller it has become more sophisticated. Lockheed Martin's stealthy F-35A Lightning II fighter is a game-changing system far more capable than the planes it will replace, but it is also more expensive to buy and maintain. While unit and operating costs are dropping, even partner nations are struggling to buy the planes they need.

As for bombers, the U.S. Air Force wants 100 B-21 Raiders to replace some of 76 aging B-52H Stratofortress and 63 B-1B Lancer bombers – both produced by Boeing – as well as 20 Northrop Grumman B-2A Spirit jets. While virtually everything about Northrop Grumman's B-21 remains highly classified, the new bomber will have less range and payload than the bombers it will replace — a concession to achieve a unit cost of $550 million ordered by Defense Secretary Robert Gates. U.S. Air Force leaders hope to control cost to acquire more than 100 new bombers to keep the B-21 from becoming a boutique force like the B-2. But some fear that even 100 new bombers will not be enough given that only 70 or so aircraft would be available at any time.

The US Air Force must also explore how it can increase manpower, invest in new capabilities and get airman back into thinking, training, and exercising to succeed in contested airspaces. It will be a major challenge. During the Afghanistan and Iraq wars, the U.S. Air Force cut fighter squadrons to grow remotely piloted aircraft (RPA) units to support global counter-insurgency operations. Aside from aircrew and maintenance personnel, analysts were needed to process imagery and intelligence. Better sensors meant analyzing each hour of imagery went from 10 to 80 hours. So great was the intelligence analysis expansion that "USAF" – an acronym for the U.S. Air Force – appeared to stand for the "US Analytical Force." Such a shift was vital, but came at the expense of combat air forces required to deter resurgent powers like China and Russia.

Meanwhile, with the rising cost of U.S.-led operations in Afghanistan and Iraq, lawmakers' reluctance to fully fund true war costs and post-financial crisis budget pressures drove dramatic program cancellations. Acquisition of Lockheed Martin's F-22 Raptor, for example, which was deemed critical to securing air superiority in advanced threat environments, was capped at 197 instead of 381 aircraft units. Other programs remained alive, but were so underfunded it could take over 150 years to recapitalize the U.S. Air Force. For example, the U.S. Air Force's 1950s-era fleet of more than 500 Boeing KC-135 Stratotanker aircraft will replaced by the Boeing's KC-46 at just 14 aircraft per year.

Acquisition of the F-22 Raptor was capped at 197 instead of 381 aircraft units. Other programs were so underfunded it could take over 150 years to recapitalize the U.S.

U.S. Air Force plans to recapitalize its geriatric fighter force with 120 new F-35s a year for the coming decade were pared to only 46 aircraft this year in the service's budget request, forcing older planes to remain in service longer with steadily higher support costs. As such, stretched modernization and, as a result, aging aircraft fleets will fundamentally hamper the U.S. Air Force's ability to sustain medium- to high-intensity combat operations in contested airspaces.

The long-running trend of acquiring fewer, more sophisticated aircraft is, however, problematic when potential adversaries are investing in systems to hold U.S. forces at risk at range and across vast areas.

China's DF-21 and DF-26 ballistic missiles can conduct pinpoint strikes on forward bases and forces or deploy bomblets and flechettes that to wreak havoc on radar and communications equipment, facilities and sophisticated combat aircraft if they are caught on the ground. Beijing understands that by damaging key radars and communications equipment as well as airbases and aircraft caught in the open, U.S. forces will be left regionally blind, deaf and powerless.

Future Force Planning

A truism in war is that equipment is always lost in greater numbers than planners expected. That was the case in Afghanistan and Iraq and will be so in a major power confrontation. Indeed, during any peer conflict, far more high-end equipment could be lost at far higher rates than anything experienced in decades. In Ukraine, Russia used massed precision surface-to-surface fires to rapidly destroy entire Ukrainian battalions, a technique China is developing on test ranges in its western deserts.

> A truism in war is that equipment is always lost in greater numbers than planners expected

America rapidly fielded a variety of systems, from armored vehicles to manned and unmanned aircraft, to save lives in Iraq and Afghanistan, but these were relatively simple. Building sophisticated new combat aircraft quickly after a future conflict starts is problematic. Prudence demands key systems be bought in sufficient numbers before a conflict, thereby potentially also serving as a deterrent.

Beijing knows that unlike during World War II when America's arsenal of democracy was able to let it produce record numbers of aircraft and ships daily from an overwhelmingly domestic industrial base. Today, U.S. commercial and military industries depend on global supply chains with just-in-time manufacture to reduce overhead costs. In a future conflict, those supply chains – some that depend on China – will inevitably be disrupted, complicating any potential accelerated wartime production efforts.

China's long-range weaponry investment is one factor in its strategy of winning without fighting – by compelling adversaries to conclude that contesting Beijing militarily would simply be too costly. China's ability to coerce its neighbors has already started an arms race that could destabilize the region. Before World War II, America debated how many aircraft would be needed should the nation go to war. Some experts argued a few thousand aircraft would suffice. As a lieutenant general commanding the Army Air Corps, Hap Arnold – who later became the five-star general commanding the Army Air Forces – countered that tens of thousands of aircraft would be needed, along with the personnel to man and maintain them, to beat Germany and Japan.By March 1844, Arnold's force was composed of 2.4 million airmen and 80,000 aircraft. More than 70 years on, Arnold's observation holds true today: "sacrifice some quality to get sufficient quantity to supply all fighting units. Never follow the mirage, looking for the perfect airplane, to a point where fighting squadrons are deficient in numbers of fighting planes."

Over time, many air forces around the world have consistently become smaller to afford more expensive systems, some shrinking so much they are struggling to muster enough crews or planes much less sustain them over prolonged periods. And as aircraft grow more expensive, users are inclined to keep them in service longer, incurring greater support costs as they age – the F-35, for example, is projected to remain in service 55 years. For their part, senior U.S. Air Force leaders say personnel cuts have left squadrons short of manpower needed to remain operationally effective. Additionally, sufficient stocks of precision munitions also remain a significant challenge.

Large and sustained defense spending increases would help the Air Force grow personnel ranks and aircraft fleets, but that is unlikely in Washington's current political environment. Therefore, Air Force leaders must continue efforts to get more for each dollar spent.

Quality Versus Quantity

To that end, it is perhaps time the United States breaks the long-established paradigm of fewer numbers of ever more costly systems by leveraging dramatic and rapid changes across manufacturing, design, autonomy, connectivity, detection, data fusion and other disciplines. Acquisition and support costs can be reduced by tightly controlling requirements, embracing open architectures, standardizing mechanical and electrical systems and making design tradeoffs bearing in mind Arnold's maxim – there is no perfect aircraft.

For some, the answer lies in building a "high-low" mix of aircraft. The novel Observation/ Attack-X program seeks to identify a new aircraft that is inexpensive to buy and maintain for use in counterinsurgency operations in permissive airspace, thereby freeing higher-end fighters for higher-end missions.

But more broadly, the nature of emerging threats demand aircraft with stealth, greater range and payload and more flexibility. Future planes must carry a range of different payloads whether for reconnaissance or long-range strike and be capable of highly autonomous operations or optional manning to operate effectively if data links U.S. forces take for granted are jammed. Aircraft that are cheaper to build and maintain will allow for larger fleets that can more easily absorb losses. No aircraft should be so expensive that users cannot afford to lose them in combat or in training. Indeed, new generations of inexpensive, unmanned, autonomous aircraft that are disposable as necessary will play a key future in military operations.

Open architectures can lower acquisition and support cost as well as ease future upgrades. Standardizing connectors on aircraft central wiring harnesses or adopting common internal systems like landing gear can increase flexibility and cut costs. Swedish company Saab has adopted a novel approach for its latest Gripen fighter, which first flew just before this year's Paris Air Show.

Photo: Lockheed Martin

The JAS 39E's combat system is like an Apple iPad with apps running systems or tailored to support specific missions – each user nation will be given an app development toolset to tailor aircraft systems to their mission needs, and will also be able to download upgrades at regular intervals to increase capability. The approach is similar to electric-car maker Tesla's, which allows a Model S to upgrade performance and range through purchased software downloads.

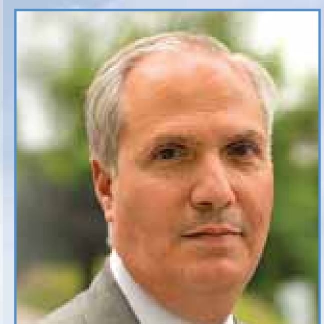
Future aero structures could be designed to last a decade or so before being entirely replaced rather than being painstakingly overhauled at enormous cost. The U.S. Air Force operates 550 KC-135s – the predecessor of the 707 jetliner – which first entered service in 1956 and the last one delivered in 1965. In the commercial world, no major airline would operate such an old aircraft fleet. High KC-135 depot costs prompted then-Air Force Secretary James Roche in 2001 to replace the oldest Stratotankers with new, leased tankers based on Boeing's 767 jetliner airframe. Congress killed the idea, and after several competitions, the U.S. Air Force eventually chose the 767 airframe as its new tanker, the KC-46.

Conclusion

The recognition that the proliferation of materials, computing, networking, communications and artificial intelligence technologies are helping America's adversaries dramatically narrow the U.S. military's edge drove the Pentagon to look to 'leap ahead' technologies for both manned and unmanned systems. The civilian world is poised for a series of major revolutions, from electric cars to truly autonomous vehicles. In turn, the defense ecosystem is reverting to its historic norm where the military adapts commercial technologies rather than the other way around. It was a post-World War II aberration that military invented many of the technologies that changed the world, whether in computing, communications or materials.

The notion of changing cost curves or imposing cost on potential adversaries is nothing new. America's potential adversaries are working hard to exploit these advantages. It is imperative that the United States and its allies move aggressively to change how they design, build and operate air systems. Failing to do so at the start of a very long period of geostrategic competition will carry major consequences far into the future. As in any competition, victory lies with the competitor who can outmatch and outlast its opponents. At the moment, when it comes to force structure and equipment, U.S. and allied governments have inadvertently stacked the deck against themselves.

Vago Muradian has been an international reporter, editor, commentator and broadcaster for nearly 25 years. For 14 years, he was the editor of Defense News and the founding host of Defense News with Vago Muradian, the world's only TV talk show dedicated to defense issues that for eight years in the Washington area and worldwide on American Forces Network. Before joining Defense News, he was the founder and managing editor of Defense Daily International and the business and international reporter for Defense Daily. He joined Defense Daily from Air Force Times, where he covered global operations, including in Europe, Haiti, Somalia and Zaire. Before covering the Air Force Times, Vago served as Defense News' land warfare reporter. He started his career at Inside the Army. At security conferences worldwide, Vago is a frequent participant and lectures on at the Defense Acquisition University. He is a member of the National Press Club and the Naval Submarine League.



Vago Muradian

Strategic Mobility and Rapid Response – Core Enabling Capabilities for Coalition Air Operations

Dr. Christian Mölling and Torben Schütz
Research Director, *German Council on Foreign Relations (DGAP) & Managing Director, Berlin Office for Defence Information*

Introduction

Air operations constitute a core element of modern military endeavours. This is true for both conventional warfare and asymmetrical warfare (e.g. counterinsurgency operations). While the former includes all kinds of different air operations like combat air patrols, close air support, air interdiction and strategic bombing, the latter mostly requires close air support for ground troops. Ad-hoc coalition air operations and the strategic mobility of aircraft, which enable a very rapid response to threats and enemy actions alike, rest on two pillars: equipment and organizations. Hence, this essay explores these pillars in more detail and tries to forecast future developments in each.

Equipment – Coalition Air Operations as ad-hoc Mixes

Specific military equipment and technologies are required to achieve strategic mobility and enable modern air operations. The strategic mobility of airborne capabilities generally depends on the availability of support aircraft, enabling them to reach their target destination, most commonly through air-to-air refuelling. Additionally, the ability to sustain air operations through airlifted logistics is paramount, since other means of transport would be too slow and thus nullify the time-saving advantages of airborne assets. Consequently, a sufficient number of air-to-air refuelling aircraft and transport aircraft are required for initial deployment. Modern full-spectrum air

Photo: U.S. Department of Defense

operations require a mixture of capabilities, ranging from intelligence, surveillance and reconnaissance (ISR) to suppression of enemy air defence (SEAD), battle damage assessment (BDA) or the communication infrastructure to distribute and relay information to strike assets in a timely manner. Only very few states are able to provide such a variety of capabilities and equipment in sufficient quantities, most notably the United States. Hence, recent coalition air operations have almost exclusively relied on US assets – for example, roughly two-thirds of air-to-air refuelling aircraft during the NATO-led Operation "Unified Protector" were provided by the Americans. It was essentially to this backbone that coalition partners' capabilities were added, mostly strike aircraft in Operations "Unified Protector" and "Inherent Resolve".

While it is crucial for coalition air operations to include as many partners as possible to broaden political support for operations, the resultant patchwork of equipment compositions lead to numerous military and technical problems. Most notably, imbalances in contributions, typically caused by capability and equipment gaps in fleets, force some partners to provide disproportional quantities of certain types of assets, especially force multipliers such as ISR or air-to-air tanker assets. If contributions exceed the contribution originally planned by a particular coalition partner, it complicates and prolongs planning and execution. Furthermore, it can endanger the political commitment and consensus among coalition partners.

As long as such a situation of disproportionate burden-sharing exists the risk for failure of coalitions and their operations remains significant. The burden may even increase when expeditionary warfare efforts meet stiff popular and political resistance in Western societies. Consequently, coalition capabilities would be enhanced if willing partners would either have similar fleet compositions in terms of capability proportions (e.g. 50% strike aircraft, 25% tankers, 25% other support aircraft) or specialized fleets, contributing specific assets to the coalition effort. Since most military equipment procurement plans can stretch over several years or even decades, time is an important factor in a state's or coalition's potential strategic shift towards more strategic mobility and expeditionary capacities.

Coalition operations can draw huge benefits from a high degree of standardisation and mutual certification in various fields, from equipment at both the systems-level and below. On the systems level, common equipment could simplify logistics of spare parts and POL's (petroleum, oils and lubricants). However, in reality, standardisation remains a huge challenge, even among NATO allies. On the sub-systems level, more detailed technical cooperation is required. One of the obstacles NATO faces in terms of equipment modernization is different modernity statuses of legacy communications equipment (Link 11 vs. Link 16/22). A lack of commonality here has grave effects on the gathering and distribution of information, which is the core element of network centric warfare and Western military superiority. Europe's efforts to build a joint air-to-air refuelling capability for example required the standardization of refuelling noses so that all aircraft types were able to refuel with all available tankers. Lastly, standardised munitions or at least standardised serial interfaces of munitions (such as for missiles and bombs) are a true asset for coalitions especially when stockpiles of some partners should run low.

In the future, it is likely that more states will have the ability to both develop and produce equipment required for modern air operations and strategic mobility as well as the ability to acquire such equipment from the international market without depending on Western or Russian suppliers. With the emergence of new defence industrial players such as China, Turkey and South Korea, and the easing of arms export restrictions on Japan, new suppliers are available in the market. Moreover, existing technologies will proliferate faster than in the past. More states are already acquiring the equipment for expeditionary air warfare, particularly air-to-air refuelling tankers and transport aircraft which, due to their relatively unproblematic character as defense exports, are becoming widely traded in the global defense market.

Further out, new technologies and their consequent application to military means could make strategic mobility and especially rapid responses much easier. While ISR data will be collected and integrated in real-time by networks of unmanned systems, nanosatellites and manned platforms, the greatest innovation will most likely occur in artificial intelligence (AI) and algorithms supporting or executing the assessment of the ever-growing data-stream. Currently, the manual analysis of incoming ISR data is one of the most serious bottlenecks in the execution of air operations. Given a sufficient communication infrastructure or computing power in transportable containers, technology solutions such as AI would significantly reduce manpower requirements in air operations and consequently in deployments.

> Faster analytics and decision-making processes **will significantly increase** the speed at which strike operations can be conducted

Faster analytics and decision-making processes will significantly increase the speed at which strike operations can be conducted. If the "Revolution in Military Affairs" was all about information superiority and driven by the escalating number of sensors, the next huge step is decision superiority - driven by the intelligent automated analysis of collected data. Furthermore, strike capabilities may change too: In the first step, manned platforms will likely remotely-control several unmanned systems and use them to lower the barriers for a forced entry by manned aircraft into contested airspaces. This combination largely resembles current logistical requirements to achieve strategic mobility, since each component is similar to current aircraft and their requirements. Soon, however, innovations in robotics, AI and miniaturization will likely lead to swarms of small unmanned systems as strike forces, which can more easily be deployed and operationally sustained – their easier storage and launch from standard ISO containers, for instance, will open up an entirely new era for militaries. Furthermore, hypersonic cruise missiles will make the world an ever-smaller place and enable even faster reaction times to imminent threats from adversaries. Both innovations will effectively make air operations less dependent on manned platforms and reduce logistics requirements, enhancing strategic mobility.

Organizations – Sharing is Caring

Coalition operations inevitably include clashes of diverging organizational structures and operational procedures. Recent NATO operations, especially Operation "Unified Protector", underlined this in various ways where problems arose, ranging from information- and intelligence-sharing to incompatible training and education of staff officers. Ultimately, the operational and tactical efficiency of air operations with precision-guided munitions depends on the quality and availability of ISR information to the staff officers in the planning cells and the strike aircraft performing the missions. Yet, here lies the most challenging problem for coalitions: to develop procedures and systems that allow for the seamless sharing of ISR information. Currently, such information-sharing might be heavily restricted or delayed between partners, depending on their political relations.

While, at least organizationally if not always technically, NATO states are able to share classified information without problems, other coalition partners might find it difficult to access data because they either do not know NATO procedures to request such data or because they are not

Photo: U.S. Air Force

allowed to access certain types of classified data. Since "NATO+" coalitions, which include a number of NATO states as well as non-NATO partners, are likely to become more numerous, this is a crucial challenge. Past operations bypassed this problem through the extensive (and successful) use of liaison officers. So far, liaison officers have served as analogue "network nodes" in an increasingly digital combat environment, which obviously limits the speed of information exchange and thus operations. Furthermore, coalition operations might be hindered by political considerations of certain partners – for example, force multipliers which are not allowed to be used by other coalition members, or politically motivated restrictions on the sharing ISR data have appeared in the past.

> Knowledge of organizational characteristics and procedures of other coalition partners requires both training and real operational experience

Knowledge of organizational characteristics and procedures of other coalition partners requires both training and real operational experience. The improvement of common procedures and the development of training courses as well as the adjunct training alone will take time, underlining the fact that ambition and achievement of strategic mobility and coalition warfare capabilities is a mid-to-long term project. Moreover, such training should not be focused on one type of air operations alone, since institutional knowledge about the efficient conduct of other types can vanish quite fast, depending on the duration of staff posts for officers.

A certain commonality in fleet structures and available aircraft certainly requires the sharing of tactical procedures and a thorough common training of crew members, such as on common air-to-air refuelling procedures. This is especially relevant for states which are working to enhance their expeditionary capabilities but are unlikely to be able or willing to execute purely national operations. Western states, as some of the most likely members of future coalitions, will have to decide how much knowledge they are willing to share with partners to potentially gain their military support in future air operations. Otherwise, they might face different structures and procedures in future coalitions – and such ignored lessons that will chip away combat effectiveness and efficiency. In the future, it is likely that the general procedural knowledge to perform expeditionary air operations will proliferate among states, as does the equipment and technologies required to create and sustain a certain level of strategic mobility for air forces. However, the diffusion of common organizational structures and procedural knowledge to enable seamless coalition air operations between partners is by no means guaranteed and depends on the political will and sustained effort of participants. Assuming that NATO remains the most capable military alliance in the near future, it is likely that it will serve as a pre-dominant blueprint in the conduct of air operations. Hence, NATO members will have to decide about the political instruments (e.g. through the various NATO partnership programs) and the depth of knowledge transfer they are willing to provide in support of coalition air operations. What is clear is that future air operations in contested airspaces are unlikely to allow for "analogue devices" like liaison officers to exchange information between partners without harsh losses in fighting power, equipment and lives. Yet the more digitalized and fluid the communication network of ISR, command and control and strike assets becomes, the more important cyber warfare becomes, which will restrict the political and military will of states to share information and digital infrastructure or take chances to compromise their networks.

Conclusion

"The age of air power", as military historian Martin van Creveld called it, was thought to be over after Western interventions such as in Serbia where it was thought subsequent counterinsurgency operations could not be won by air power alone. Yet today, air operations are still one of the primary means of states and coalitions to intervene in conflicts according to their strategic and political interests. This is not only due to the comparatively low risk for their own forces, but also because air assets can, if circumstances permit, serve as rapid response forces, as seen in the short-term Western intervention to support Kurdish resistance against the so-called Islamic State in Kobane, Syria, and west of Erbil, Iraq, in 2014. Strategic mobility, ensured through the right military equipment and organizational knowledge, greatly enhances a state's options to engage in conflicts, whether it does this alone or with coalition partners. The future will likely see more states harnessing modern strategic mobility capabilities for their air forces. Inherently, this increases strategic instability, if not checked through close peer-to-peer (between states or coalitions alike) communication efforts. Syria might serve as an early example in this respect, where there are confrontations between aircraft from a dozen or more states, which are not necessarily on the same side of the conflict.

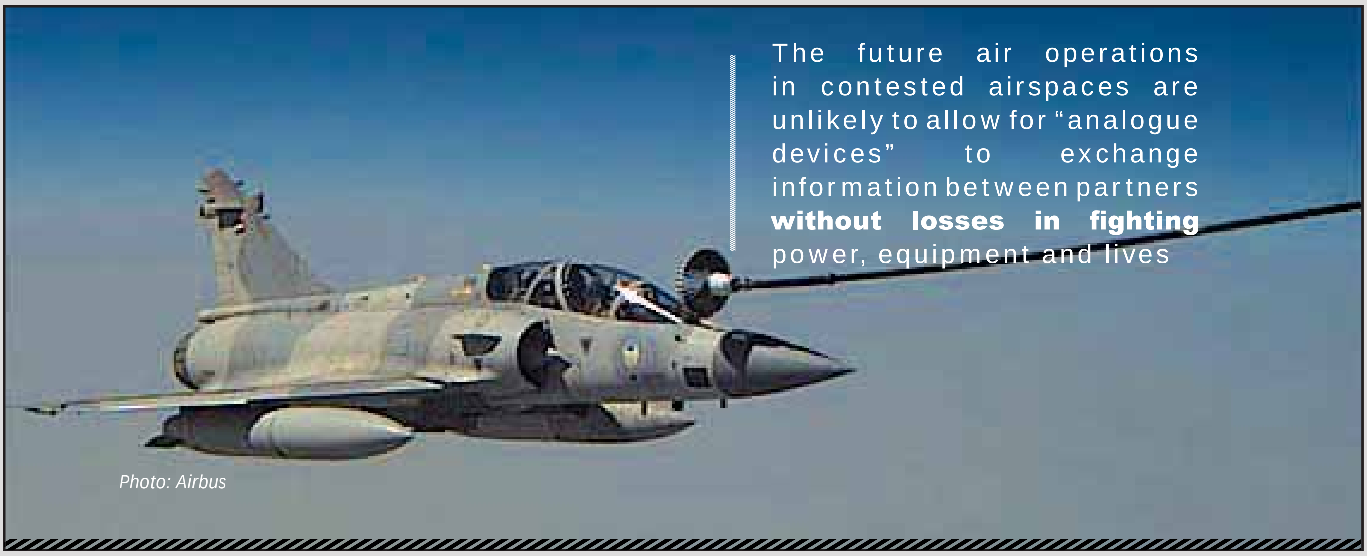


Photo: Airbus

Dr. Christian Mölling is Research Director at the German Council on Foreign Relations (DGAP) in Berlin, Germany. Besides managing the strategic positioning of the DGAP, he leads DGAP's work on security, defense and defense industrial issues. Prior to DGAP, Christian held research and leadership positions with the German Marshall Fund of the United States (GMF), the International Security Division at SWP, the German Institute for International and Security Affairs, the Center for Security Studies in Zurich, Switzerland, and the Hamburg Institute for Peace Research and Security Policy. Christian has been visiting fellow to the EU Institute for Security Studies in Paris, France, the Royal United Services Institute in London, UK, and the Fondation pour la Recherche StratÈgique in Paris, France. He studied Politics, Economics and History at the Universities of Duisburg and Warwick University and holds a doctoral degree from Ludwig-Maximilian, University Munich, Germany.

Dr. Christian Mölling

Torben Schütz is the Managing Director of the Berlin Office for Defense Information. His work as a political advisor focuses on military capabilities, military technology and innovation and the defense industry. Before taking up this position, he worked for three years as a research assistant in the International Security Division at the German Institute for International Affairs and Security (SWP) in Berlin, Germany. While there, he was engaged in the "European Defense Monitoring" (EDM) and "Permanent Monitoring and Analysis of military capabilities and Defense sector trends" (PMA) projects – both financed by the European Defense Agency (EDA). In the framework of these projects, he conducted several in-depth studies on unmanned aerial systems, armoured vehicles, ground-based air defense and maritime capabilities across Europe. He holds a MA degree in political science from Leibniz University Hanover.

Torben Schütz

C4I and the challenges of a Coalition Environment

Douglas Barrie
Senior Fellow for Military Aerospace, *The International Institute for Strategic Studies (IISS)*

Command, Control (C2) and Connectivity in the Air Domain

If wars could be won by the number of lighting-bolts on PowerPoint presentation slides, then simply illustrating connectivity would be an extraordinary deterrent. Unfortunately this is not the case, and the political exercise of military power still demands the expenditure of "blood and treasure".

As is the sometime the military's want, it is prone to jargon and acronyms, perhaps no more so, ironically, than in communications. Command, Control, Communications, Computers and Intelligence, C4I in its abbreviated form, conflates the human and technological elements of military endeavour, while the last three (communications, computers and intelligence) are facilitators for the first two (command and control).

Effective command and control when combined with the appropriate strategic, theatre and tactical aims underpins the execution of any plan of action. A key element of command and control is the capacity to convey orders and information in a timely fashion to the force or forces being deployed, coupled with the ability to flex any plan of action in response to the actions of an opponent. It is also worth keeping in mind that the Power Point lighting-bolts need to be bi-directional, conveying data, information and actionable intelligence back up the command chain.

Command and control in the air domain is a fundamental element of the effective exercise of air power. The very nature of the domain also places an emphasis on what some militaries describe broadly as "mission command". The utility of modern air power provides senior commanders with the ability to craft plans with missions ranging potentially across the whole of an opponent's geographical territory, with the assets to be involved based hundreds, or in some cases, thousands of kilometres from a discrete theatre of operations. Two of the guiding tenets of mission command are decentralisation, and timely and effective decision-making. Any C4I system should enable and support the leadership

Photo: Al Jundi Journal

in achieving their military objectives, but it should not be viewed as a replacement for leadership. Process is not a substitute for intellect.

Embedded within the language of C4I is of course the underpinning technology that is computers, or more broadly the digital 'revolution'. Digitisation has and continues to have a profound effect on how war is waged, almost irrespective of the nature of the conflict itself. Insurgents in Afghanistan, Iraq, and Syria have embraced the use of digital systems, for example in the guise of mobile phones being used to detonate remotely improvised explosive devices, or at the level of influence in their use of social media for propaganda purposes. Allied states, meanwhile, have increasingly operated within and exploited a networked environment in attempting to meet military aims and political goals.

C4I in the Air Domain

Concepts such as the 1990s "Revolution in Military Affairs" and "Network-Centric Warfare" in essence were arguably attempts to conceptualise and capture the impact of digital technology in the military domain. For air power practitioners much within both sets of ideas would have been familiar. Air was an early adopter of the computer in its analogue guise, while the very nature of air warfare requires a networked approach to maximise effectiveness. Concentration of force, offensive or defensive, at distance and over time requires management, or in military parlance command and control. Familiarity, however, does not necessarily imply simplicity or mastery, at the service, national or multinational environment.

Interoperability, open architectures and systems commonality, like lightning-bolts, are the stuff of presentation slides, and also underpin effective command, control and communications. Transferring such worthy aims into practice, however, has and remains a challenge at all levels of the military, single service, joint commands, and in the coalition environment.

Multilingual Demands

Within the bounds of a single service, even the best equipped, interoperability in terms of elements of C4I remains a problem. The USAF's two 5th generation combat aircraft, the F-22 and the F-35 are fitted with different tactical data links that are incompatible. The F-22 is equipped with the Intra-Flight Data Link. This is a low probability of detection, low probability of intercept datalink with which F-22 pilots can communicate with other F-22 aircraft. The F-35 uses the Multifunction Advanced Data Link, which is not compatible with the F-22 system. In turn neither of these are directly backward compatible with data links fitted presently to fourth-generation combat aircraft that remain in the inventory, such as the F-15 and F-16 aircraft.

Fourth-generation aircraft use Link 16. These shortcomings have been recognised and work is underway to provide gateways that will allow cross platform data link communication, allowing the undoubted sensor capabilities of the F-22 and F-35 aircraft to be exploited better in terms of situational awareness for broader U.S. forces involved in any cooperative mission, and to build an improved intelligence picture of an opponent's activities and force disposition.

Link 16's design heritage can be traced back to the late 1970s. While it has now been widely adopted, and is of considerable value, its architecture is such that it is increasingly ill-suited to a net-enabled C4I construct. The Link 16 messaging structure is restrictive, while there are also limitations to the way in which a network is managed using the Time Domain Multiple Access construct. The effect is that the air force has to rely on a sub-optimal data-link architecture within its fast-jet fleet.

This lack of compatibility is far from the exclusive purview of the United States Air Force. The United States Army and United States Navy face similar challenges in areas such as communications architectures at the service and joint - or Purple - levels. This is a problem that is only compounded when one considers a coalition environment.

It's Good To Talk

Link 16, however, is not without advantages, arguably the most important being its near ubiquity. This messaging standard is used widely within NATO and also by a number of other nations that purchase military equipment from the Americans. As such, and irrespective of its limitations, this makes 5th to 4th generation connectivity exploiting Link 16 an understandable aim. In an Alliance context this is given greater importance considering several F-35 aircraft operators other than the U.S. will operate the aircraft in conjunction with so-called legacy types such as the Eurofighter Typhoon and Boeing F/A/18-E/F. The aptly-named Babel Fish III trial, held in early 2017, was intended to demonstrate datalink connectivity between British Typhoon and the F-35B.

> The Link 16 messaging structure is restrictive, while there are also limitations to the way in which a network is managed using the Time Domain Multiple Access construct

The trial was carried out as part of Exercise 'High Rider'. Targeting data from the F-35 sensor suite was provided to Typhoon aircraft via data link during the trials. Connectivity was provided by using gateway software developed under a United States Air Force Joint Capability Technology Demonstration programme demonstrated first in 2014.

Wicked Problem

Recognising you have an issue is the first step in addressing it, and there is certainly no question as to whether the challenges of C4I interoperability at a coalition level have been recognised. Addressing these, however, remains demanding, with a number of factors contributing to what is a 'wicked problem.' The pace of change in the commercial computer sector in itself poses a difficulty for the military. Computer hardware obsolescence is measured in terms of a few years in the commercial world, while for the military, platform obsolescence it is measured in terms of several decades. And it is now the commercial sector, rather than the military, where the majority of digital innovation is occurring. How to make best use of such innovation, while accommodating the far greater longevity of combat aircraft or command and control infrastructure is a challenge.

The U.S. and its coalition partners have recent experience of C4I in a real-world operational environment. Air operations in Afghanistan, Iraq and Libya have involved multiple NATO and non-alliance nations. The Libyan air effort in operational terms was a success, although the wider political outcome has resulted in what is for the moment a failed state. In the air domain, however, the operation also served to underscore the shortcomings and challenges the NATO alliance continues to be confronted by with regard to multiple elements of the command and control, communications, computers and intelligence architecture. The shift from the U.S.-led Odyssey Dawn to NATO's Unified Protector revealed the continuing challenges of coalition operations. In terms of physical infrastructure the NATO Combined Air Operations Centre (CAOC) in Italy was initially inadequate, as was communications. Interoperability issues also surfaced quickly. In Afghanistan the previously mentioned limitations of Link 16 were also apparent.

To suggest that coalition partners simply had to make do and mend in these wars in dealing with the aforementioned C4I difficulties would be to do a disservice to their ingenuity and perseverance in delivering the desired air powers effects where the communications, digital architecture and the infrastructure to support these was far from ideal. In all three conflicts, however, coalition forces had the benefit of facing an opponent unable to contest the air domain, or to mount any meaningful challenge across the electro-magnetic spectrum or in the cyber domain. This is a comparative luxury that can no longer be taken for granted. As the security environment has deteriorated then the risk of war with a near-peer or peer competitor is no longer a near impossibility, though thankfully remains unlikely.

> A 'net-enabled' capability also allows for the possibility of a net-disabled outcome

A 'net-enabled' capability also allows for the possibility of a net-disabled outcome. Peer and near-peer competitors have watched how the U.S. and its allies have waged recent wars, exploiting the overwhelming U.S. dominance in the air domain, built in considerable part around the benefits of digitisation. The electro-magnetic spectrum upon which much C4I capacity rests would almost certainly be highly contested in any conflict with a peer or near-peer or nation-state. Redundancy and robustness will become even more important for friendly force digital infrastructure and systems. Russia, for example, continues to develop a wide variety of electronic warfare capabilities intended to deny or degrade the performance of C4I systems, while at the same time it looks to better exploit its own net-enabled capabilities, similarly with regard to China.

The U.S. and allies continue to face a nested problem with regard to C4I and interoperability. Within the U.S. each service continues to address internal issues, while all also grappling with inter-service interoperability. The challenge for both the US and its allies is trying to identify a route to ensuring that any cross-domain, inter-service solution, or more likely solutions, can also be used by partner nations.

Photo: Al Jundi Journal

Douglas Barrie is the Senior Fellow for Military Aerospace at the International Institute for Strategic Studies (IISS). His interest include Russian and Chinese air power, and guided-weaponry. He joined the IISS in 2010 following a career as a defense-aerospace journalist during which time he worked for Jane's Defense Weekly, Flight International, Defense News, and for the ten years prior to joining the IISS with Aviation Week & Space Technology.

Douglas Barrie

A UAE Perspective on Transformation to Network Centric Operations (NCO)

Major General (Ret.) Khalid Abdullah Al Bu Ainnain
Former Commander, *UAE Air Force and Air Defense*

Strategic Background

The UAE's ongoing involvement in the Saudi-led military intervention in Yemen is the latest of various recent experiences emphasizing the need for real-time operational connectivity for the Air Force, especially, and militaries at large when executing coalition or Joint operations. The Saudi-led military intervention in Yemen, which brought together a coalition of militaries to execute sustained operations from forward-operating bases in-theatre as well as main operating bases and operation centers situated in the home territories of coalition partners, constantly confronted complex challenges as far as interoperability and the end-to-end force connectivity that underpins true unity of effort were concerned.

The experience of the Saudi-led coalition in Yemen reflect the broader realities of the 21st century security environment which has complicated defense planning. Military capability must increasingly be able counter a growing range of old and emergent threats – including armed non-state actors and transnational criminal networks, failed or failing states, weapons of mass destruction (WMDs), advanced missiles, and cyberattack. Space and remotely piloted aircraft (RPA) provisioning intelligence, surveillance, tracking and reconnaissance (ISTAR) are becoming the latest frontier for military competition as they take their place as the ultimate high-ground for military intelligence – able to provide round-the-clock imagery intelligence (IMINT), 3-D mapping, ground moving target indication (GMTI), and stand-off targeting support.

Faced with a 24-hour attack possibility, the Air Force – and indeed militaries at large – can be threatened with a range of threats – WMDs, tactical ballistic missiles (TBMs), supersonic high/low altitude cruise missiles, anti-radiation missiles, high/low altitude bombers, and a range of advanced precision-guided weapons and precision-guided "kamakazi" drones. Further complicating the threat environment are stand-off jamming aircraft, advanced self-protection systems, smart decoys, RPA – low altitude tactical variants as well as high-altitude slow-speed lurking vehicles – and loitering electronic warfare or 'special missions' aircraft. Yemen of course has not posited us with the full spectrum of the threats characterizing the current threat environment but its experience has demonstrated some salient features of this, particularly how armed non-state actors can take control and hold large territories through hybrid warfare by combining classical counter-insurgency tactics, techniques and procedures (TTPs) with technologies such as tactical RPAs, TBMs, and fairly robust supporting command and control (C2) often associated with conventional militaries.

Photo: Wam

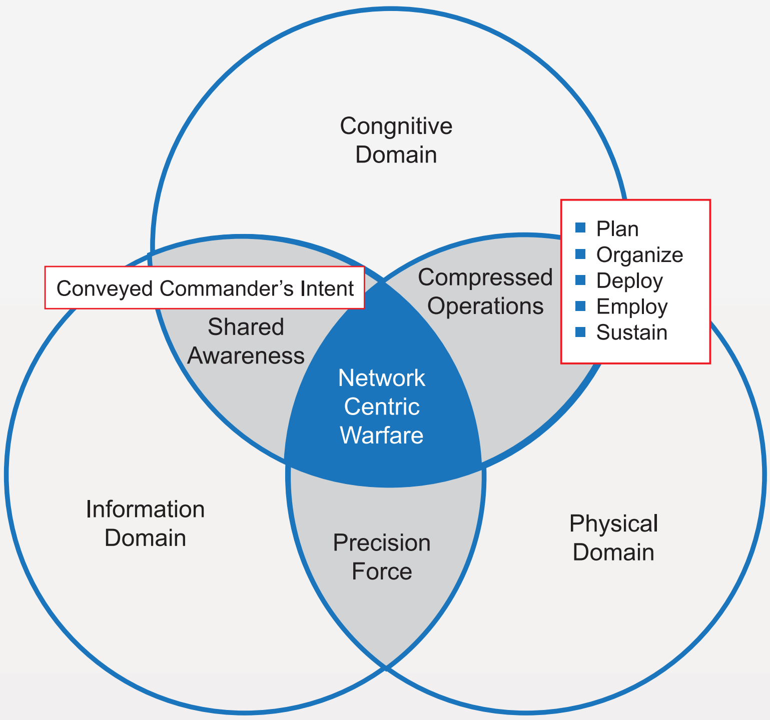
Defense at large is now moving into a new strategic environment as threats become more varied, more numerous, increasingly well-equipped, and more flexible. Recent approaches of prioritizing quality over quantity, though still important, will no longer be sufficient in themselves. The emergent challenge for defense at large and the Air Force especially is in being able to effectively operate within the decision-cycle times of adversaries. In doing so, defense strategy will continue to be built on "**qualitative**" advantages though approaches to capability development now will no longer be based on platform-centric superiority but network-centric operations (NCO) as a way to make forces better connected – and by extension, more adaptive and more flexible – in the battlespace. NCO is logically coupled with effects-based operations approaches (EBOA) because while one emphasizes situational awareness and understanding – the enabler – the other focuses on the outcomes of achieving and exploiting such informational superiority – the effects. NCO effectively means reorienting away from platform-centric operations towards a network of interconnected platforms to produce a sum that is greater than its parts.

> The emergent challenge for defense and air forces in particular will be to effectively operate within the decision-cycle times of adversaries

NCO as a Concept of Operations

The most crucial challenge for the Air Force and Air Defence, like other services, is a residual one and relates to how effectively they are able to gather, process, fuse and integrate ISTAR in support of time critical targeting. Essentially, air forces are seek to plan and execute the 'F2T2EA' loop ("find, fix, track, target, engage and assess") as close to

Information Age Warfare



near real-time as possible. Throughout Saudi-led coalition operations undertaken in Yemen, closing the F2T2EA loop has remained a constant challenge for Commanders and operators as they faced non-conventional and fragmented forces – as the case has been in any major military intervention in recent times, from Iraq to Libya to Syria.

Today there is greater appreciation than ever in the agility and connectivity provided by rapid information-sharing that can translate into improved responsiveness for operations, in information-gathering, and – crucially – in decision-making at all levels of command. The level of information superiority that is underpinned by rapid end-to-end information-sharing can create a "decisive combat advantage" because when geographically dispersed forces are able to achieve a high level of 'shared' battlespace awareness they have the capability to self-synchronize to achieve the Commander's intent. But information in itself is not power – it only becomes so when it is effectively collected, processed, fused, unified, disseminated, and used at the right time, at all levels of command and whenever needed.

NCO is about achieving information superiority through utilizing and exploiting information-sharing at virtually all levels of the force – enabling information flows vertically from strategic to operational and tactical levels to provide an integrated and transparent flow of information that connects all command and control (C2) processes between commanders, operational planners, deployed and frontline forces. Fundamentally, NCO is about using cooperative efforts to bring together distributed warfighting capabilities and projecting the desired effect in the right place at the right time.

The Saudi-led military intervention in Yemen has demonstrated the need and importance of real-time regional operational connectivity to engage highly dynamic targets. Greater speed in gathering and sharing information shortens decision-time cycles of adversaries and, in the perfect scenario, allows 'us,' 'green' or 'friendly' forces to 'act' while adversaries are still planning and organizing. Operations conducted in Yemen have demonstrated to the Saudi-led coalition the importance of reducing planning cycles from 24-hours to under a few hours and of rapid adaptation in responding to threats. In the perfect scenario, highly robust NCO would enable planning in real-time within a few years. Such benefits are a strategic 'game-changer' as we know threats such as tactical ballistic missiles – responding to which requires time-critical decision-making – require commanders, warfighters, and automated weapon systems and C2 to have assured access to high-quality information in order to respond quickly and decisively.

NCO can involve many dimensions but, more than anything, it is the approach to developing

NCO-Enabled Transformations

Situational Awareness	Situational Understanding
Need to Know	Need to Share
Battlefield Command	Battlefield Management
Operation Centers	Battle Management Centers

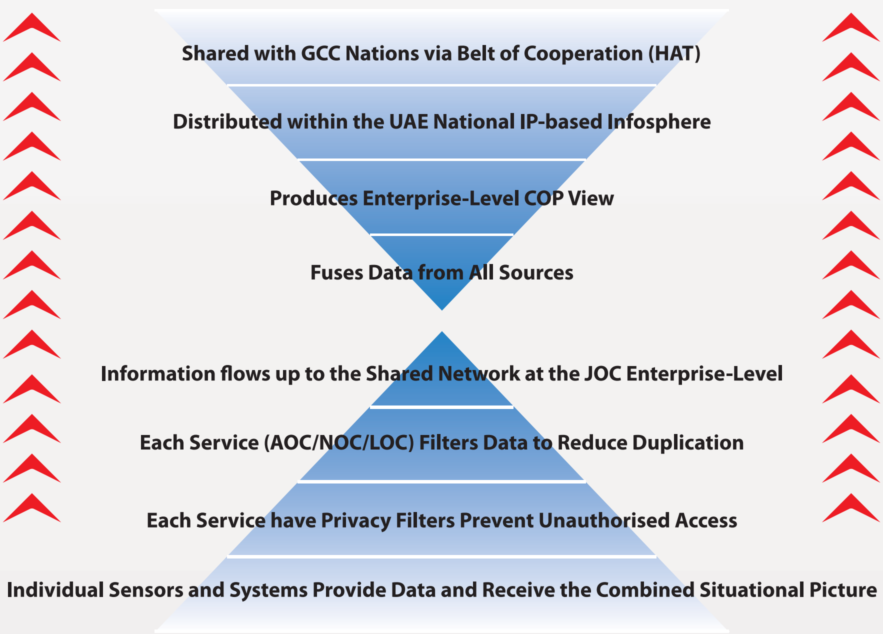
a concept of operations (CONOPS) to provide the right data to the right person at the right time. Technology will force us into this more efficient future especially taking the benefit of commercial-off-the-shelf (COTS) technologies, especially internet protocol (IP), for better connectivity's – future generations may look back to study our ways today and be baffled by why we stored ISTAR, operational, technical, and logistical information on different databases that were not connected together to enable near-real time information-sharing between platforms or the personnel operating or supporting them even when the enabling technology to do so was available and sufficiently mature. But of course the core challenge in transforming to NCO is not purely or even largely technical – it is more inherently cultural and relates to changing the mindset of our planners and commanders. As far as NCO is a CONOPS it rests on achieving a change with cultural mindsets on how we approach the collection, processing, use, and sharing of information in support of collaborative planning, for interoperating with force elements, and achieving optimum unity of effort in support of the Commander's intent.

> NCO is the approach to developing a concept of operations (CONCOPS) to provide the right data to the right person at the right time

Key Elements of NCO Capability

Today's *infosphere* – a term referencing the technology and processes to collect, process, fuse, unify, and disseminate information – remains limited as far as our operational application of it is concerned. For us in UAE, moving forwards progress will become possible because of both the greater accessibility of technology, technical expertise and as such a transformation becomes more greatly recognized as being fundamental to our security in the future. 'Across-the-force' network connectivity is an over-the-horizon

Information Fusion Process



opportunity that we will inevitably need to adopt – it will enable planning and operations to focus on the 'effects' needed to achieve military, political or strategic outcomes in ways we have only imagined until now. However our institutional behaviors, individual and leadership mindsets, and cultural resistance to change will decide how quickly we will be able to exploit the true power of NCO.

> The Air Force and Air defense and militaries at large, in fact, will need to shift from traditional 'need to know' approaches for information-sharing towards 'need to share' approaches where, like the internet, a 'many to many' protocol for information-sharing is established

Here, the information consumer – the forces at large – will have simultaneous access to 'many' information-providers, and information-providers can 'provide' information to 'many' users at the same time. Secured network-connectivity will mean users can 'find and pull' required information that is visible, accessible, and understandable in near-real time.

In such an "Enterprise Secured Services" environment, commanders, operators, warfighters, support personnel – in fact decision-makers at all levels of the command hierarchy – together with sensors, intelligence, operators and weapon systems will be seamlessly networked together. With such Enterprise Secured Services, Joint forces will be able to operate in highly complex environments where deployed tactical users can collaborate in near-real time through standard operating procedures (SOP) without extensive communications planning prior to initiating operations. As soon as the correlation and synchronization – at once – of different operational tasks for air, land, and naval forces is achieved, such a degree of 'connectivity' at the Joint level becomes a reality.

Our UAE Armed Forces commanders and planners should think of the infosphere essentially as a "network of networks" where nodes can work in a "plug and play" fashion with "find and pull" capabilities, because common modes of communication and exchange of data, voice and video are already established and in place. In UAE most of our currently deployed national network and assets are fully IP-based with controlled and secure access – this foundation could provide the infosphere needed to service a complete situational overview of the entire battlefield and rapid scalability from tactical to strategic levels. Such a network is capable of linking our fixed and mobile platforms via self-organizing networks sharing near-real time information both inside and outside UAE borders.

Together with converged data, voice, video and imagery in a high-capacity and sufficiently secure mode, mission-critical communication requirements could be supported around a fixed or ad-hoc system that is adaptive, dynamic and self-reconfiguring. With forces able to use multiple network protocols (such as secure Ethernet, ATM, and WAP) for services and applications with standardized interfaces, command and control "on the move" could be enabled – meaning UAE forces deployed inside or outside the country could become smaller yet more highly mobile and more lethal. Using commercial-off-the-shelf IP open standard architectures for developing such a network would provide multiple advantages with their easier, cheaper and faster-to-implement offering and full scalability – providing the ability to add platforms and units into the network without necessarily adding to its inert complexity or to the processes of creating new services and applications on-demand.

By utilizing the benefits of open standards, our military planners can help secure high-speed IP services and deliver end-to-end network connectivity for forces throughout thereby making it possible to adapt quickly and more dynamically to changing operational requirements without disrupting existing services. Moreover, a highly flexible communications, computing, and information infrastructure achieved through

"Machine-to-Machine" connectivity that is able to dynamically allocate resources such as bandwidth, spectrum, computing power and rerouting based on mission requirements and use of precedence, priority and resource allocation techniques would deliver the responsivity needed by our forces for meeting constantly changing operational needs.

The sort of strategic transformation required to exploit NCO is an iterative process and the Air Force and Air Defense attempting to harness NCO across-the-force may find that 'data drought' can quickly become a 'data deluge' – at least in the early stages. Managing information fusion is critical to managing the challenges of potential data deluges a 'network-of-networks' may generate. As far as whole-of-force NCO is concerned the most sensible approach is for information fusion to occur within each functional operations center (air, land, naval) before flowing to the Joint Operations Center (JOC) where information de-confliction and unification takes place and from where an enterprise-level common operation picture (COP) is created and shared back 'downwards.'

In addition to providing an enabling framework to achieve interoperability, the infosphere needs to provide secure assurance and trust that the right information to accomplish assigned tasks or missions is available when and where needed in a form that all services, units and warfighting platforms can understand, use, and act on with confidence. Users would be able to access the latest, most accurate and relevant information through tremendously expanded sources to achieve a true common operational picture (COP) and thereby draw common conclusions, execute compatible decisions and take the best-informed actions that exist in their decision-spaces. When we successfully achieve rapid and transparent information-sharing with all users, anytime, anywhere, we would be able to harvest the benefits of rapid collaborative decision-making and a force that is able to self-synchronize around the Commander's intent.

A Roadmap for the UAE Armed Forces

Thanks to our leadership, the UAE Armed Forces have undergone rapid and wide-ranging

Photo: Al Jundi Journal

modernization over the past decade across its service commands with doctrine, equipment, CONOPS, training, and logistics, among other defense lines of development – the war in Yemen has demonstrated the true importance of these investments. In particular, the UAE Air Force and Air Defense, which has been a central focus of investment for capability development, has assumed important responsibilities in various recent coalitions operations in Libya, Iraq and, more extensively, in Yemen. The UAE Armed Forces have demonstrated through a variety of sustained operations outside the UAE their ability to execute combined, joint, and coalition operations with high effectiveness and precision across varying operational tempos and environments.

As the regional threat environment continues to evolve and as the UAE together with its partners in the region and more widely around the world draw lessons learned from their latest operational experiences especially in Yemen, the benefits and requirements for truly 'networked' capabilities – across-the-force, and where and when possible, across partners – have never been more greatly appreciated and needed. An NCO architecture for the UAE Armed Forces would seek to link together the AOC, LOC, and NOC to the JOC for better connectivity. The UAE's existing ground-based C4I network – 'Al Sheryan' – must be upgraded with COTS technologies to create a "secure intra-net" on the ground and in the air that can deliver the necessary bandwidth, speed, reduced latency for rapid, converged voice, data, and video information-sharing.

The challenge with effectively upgrading current UAE Armed Forces C4I network, lies in being able to deliver better quality, security, and assurance together with reach because military users at all levels have high


Photo: Mubadala

sensitivity to errors with both information and related execution. Again, just as transforming towards NCO hinges not just on technology acquisition and upgrades, or systems and platform interoperability, so too successful execution of NCO depends on users being reprogrammed to operate in a way that they collect, create and share information into the network, and in exploiting that network as effectively as possible.

In the years ahead, YahSat – the UAE's communications satellite – will fill a strategic gap by providing the UAE Armed Forces with IP-over-satellite and thereby enabling regional network capabilities for mobile command centers, aircraft, vehicles, and vessels at broadband speeds. Together with other elements of strategic assets that will underpin NCO, YahSat will play the most crucial role in placing truly the 5th generation capabilities at the doorstep of the UAE military. YahSat's network development should enable the UAE Armed Forces units to detect other systems operating in the region and automatically set their own network or sensors to appropriate frequencies – meaning that as forces move or other participants join the battlespace, systems can automatically adapt.

New capabilities and services YahSat will provide over the next decade deliver the UAE and its partners a gateway for delivering "whole-of-force" connectivity and seamless integration to underpin the interoperability required to execute combined, joint and coalition operations in real time and with the greatest effectiveness possible. As such the development of YahSat's capabilities and the future transformation of the UAE Armed Forces fully towards NCO heralds a new future horizon not only for the our Armed Forces in the UAE but also for key regional partners with whom the UAE must work collectively together with to meet shared objectives in the years ahead.

For further reading on the subject and vision laid out in this paper, you can access "Special Report No.5: A Vision for Transforming UAE Armed Forces Into Network Centric Operations", written by the same author, from www.inegma.com/uaenco.pdf

Major General (Ret.) Khaled Abdullah Al Bu-Ainnain is a former Commander of the UAE Air Force and Air Defense who retired from service in 2006 following an illustrious career spanning 32 years. During his time in service, MG (Ret.) Khaled held numerous staff and command positions, and participated in both Gulf Wars. MG (Ret.) Khaled has taken part in various high-level bilateral negotiations on behalf of the UAE and led several multi-billion dollar programs including acquisition of advanced military aircraft and land- and spacebased systems for C4I, ISR, IT, remote-sensing, flight test centers, war gaming and simulation needs. MG (Ret.) Khaled established the first Air Warfare Center in the UAE and was instrumental in the creation and development of the UAE's earliest R&D faculties. MG (Ret.) Khaled received 25 awards and decorations from the UAE and other nations over the course of his career.

Major General (Ret.) Khaled Abdullah Al Bu-Ainnain

ISR Challenges against Asymmetric Threats and Plugging Gaps in the Sensor-Shooter Network

David A. Deptula, Lieutenant General, USAF (Ret.)
Dean, *Mitchell Institute for Aerospace Studies*

Network-Centrism and the 'Combat Cloud'

Today, wireless connectivity, personal computing devices, and cloud-based applications are integral to daily life. The ability to access, process, and disseminate volumes of information anywhere, anytime has revolutionized the way the world functions. These developments are also altering the way militaries can project power. Faster and more capable networks and computing capabilities are turning information into the dominant factor in modern warfare.

Given this reality, it is critical to acknowledge that information and its management is just as important today as the traditional tools of hard military power. Information is the force evolving the traditional tools of war from isolated instruments of power into a highly integrated enterprise where the exchange of information will determine success or failure in twenty-first century warfare. Whether against asymmetric threats, or more capable existential threats, the needs are the same; delivering actionable knowledge to an effective sensor-shooter network though intelligence provided by optimal surveillance and reconnaissance. This challenge has major implications for key focus areas like doctrine, organization, training, materiel acquisition and sustainment, along with command and control.

We are at a critical juncture in history – at the center of an "Information in War Revolution" – one where the speed of information, advance of technology, and designs of organizations are merging to change the way we operate. This change has dramatically shortened decision and reaction times, and reduced the number of systems it takes to achieve desired effects—to include on the part of our adversaries. Where it used to take months and thousands of airmen and aircraft with separate functions to attack a single target, today we can find, fix, and finish a target from a single aircraft within minutes. Moreover, one of the most common techniques of "asymmetric threats" today is their innovative use of commercial off the shelf (COTS) technologies to form intelligence, surveillance and reconnaissance (ISR) networks of their own to enable an enhancement of their decision cycle.

Ever since the introduction of mechanized technology in the early twentieth century, the scale and scope of combat has been governed by industrial means of power projection. Advances in aircraft, ships and ground vehicles increased speed, reach and precision but still relied on mass-in-force application. In the last century, military missions, historically restricted to land and sea, expanded into the air, space, and underwater domains. However, the ability to project power globally was wholly dependent upon mechanized technology.

> Advancements in computing and network capabilities are empowering information's ascent as a dominant factor in warfare

In the twenty-first century we face another technology-driven inflection point that will fundamentally reshape what it means to project power. Advancements in computing and network capabilities are empowering information's ascent as a dominant factor in warfare. No longer will it be sufficient to focus on just managing the physical elements of a conflict – planes, satellites, troops, amphibious elements or ships at sea – for these individual platforms are evolving from a stove-piped, parochial service alignment in a loosely federated "joint and combined" construct today to a highly integrated enterprise collaboratively leveraged through the broad exchange of information. Said another way, desired effects will increasingly be attained through the interaction of multiple systems, each one sharing information and empowering each another in support of a common purpose. This phenomenon is not restricted to an individual technology or system and nor is it isolated to a specific service, domain or task.

It is a concept that can be envisioned as a "combat cloud" – an operating paradigm where intelligence, surveillance and reconnaissance (ISR), data management, connectivity, and command and control are core mission priorities. While mechanical technology will continue to serve as a key factor in future military operations, the information empowering these systems will stand as the backbone maximizing their potential. As the combat cloud is developed, it promises to transform an expansive, highly redundant defense complex with radically enhanced ISR gathering, processing and dissemination capabilities. These attributes will offer actors at every level of war dramatically enhanced situational awareness by transforming masses of disparate data into decision-quality knowledge.

A Vision for the 'Combat Cloud'

This represents an evolution whereby individually networked platforms transform into a broader system of systems enterprise integrated through domain and mission agnostic information linkages. A distributed, self-forming, all-domain combat cloud that is difficult to attack and self-healing if attacked, significantly complicates an enemy's planning and will compel it to dedicate more resources toward its defense and offense. In its ultimate instantiation, it will be strategically dislocating to any challenger; provide conventional deterrence to a degree heretofore

Photo: Thalesgroup

only achieved by nuclear deterrence and will enable the attainment of operational dominance in multiple domains.

Turning this vision into reality will require a significant effort for while many militaries are evolving toward informationized' forces, the integration and assimilation of related capabilities is incomplete. Forces are still predominantly organized, trained and equipped to fight a mechanized war – one in which information integration is a secondary support function.

> Forces are still predominantly organized, trained and **equipped to fight a** mechanized war

Most bureaucratic organizations and current programs reflect linear extrapolation of combined arms warfare from the industrial age of warfare. Program oversight efforts within defense ministries and governments are also lagging with antiquated industrial age governance systems impeding information-age endeavors. Any assessment of the likely landscape of future conflict must recognize no matter what the type of engagement, the outcome will increasingly be determined by which side is better equipped and organized to gather, process, disseminate and control information.

If peace-loving allies are going to win the next war, we need to gain persistent access to ISR networks while denying this same capability to any adversary. To be serious about this effort, military services need to embrace doctrinal and concept changes to how their forces are organized, trained and equipped. The concept of the combat cloud stands as a framework to empower this vision.
The concept has as its basis allied militaries linking information-age aerospace systems with cyber-, sea-, and land-based capabilities in ways that will enhance their combined effectiveness, while compensating for the vulnerabilities of each. The combat cloud concept is somewhat analogous to "cloud computing," which is based on using networks to rapidly share information across a highly distributed system of systems. However, instead of combining the computing power of multiple servers, a combat cloud will capitalize on the ubiquitous and seamless sharing of information among weapon systems – exploiting their inherent sensor capabilities – in multiple domains to rapidly exchange data to act as a cohesive whole.

Enabled by secure, jam- and intrusion-proof, multi-mode connectivity, a combat cloud may be capable of employing fewer modern combat systems to achieve higher levels of effectiveness across larger areas of influence compared to legacy operational concepts. For example, instead of relying on traditional approaches that combine mass fighters, bombers and supporting aircraft into strike packages to attack particular targets, a combat cloud could integrate complementary capabilities into a single, combined "weapons system" to conduct disaggregated, distributed operations over an entire operational area.

The combat cloud requires treating every platform as a sensor as well as an "effector." It requires a command and control (C2) and ISR paradigm that enables automatic linking in much the same way that cell-phone technology does today. It also requires seamless data transfer data without need for human interaction between the combat cloud nodes in a manner that is reliable, secure and jam-proof. While the overarching notion of actualizing a combat cloud with the degree of integration required to achieve a self-forming, self-healing complex is a new idea, many of the individual technological elements required to manifest this vision already exist or are under development. But each was developed in the absence of an overarching, integrating vision. In fact, each comes with a somewhat different operating concept that is unique to particular systems.

While delivering distinctive capabilities, countries and services developed networks in a stand-alone manner without an overarching construct to ensure joint or allied partner interoperability – much less interdependency. Establishing the combat cloud as the operational template for the various linkages provides a basis to achieve interoperability and interdependency goals with existing systems as well as to guide development on emerging programs and establishing a guiding framework for common requirements. Current systems are largely expected to operate in a semi-autonomous fashion with a basic level of collaboration with other platforms, creating shortcomings that place pressure on individual assets to possess numerous internal capabilities. The complexity inherent to this approach drives lengthy development cycles, which in turn leads to requirement creep, time and cost overruns as well as delays in delivering capability to frontline commanders.

> Individual platforms no longer need to leverage as much from their internal attributes

In sharp contrast, the combat cloud can enable individual platforms to harvest a wide range of capabilities by sharing critical information and thereby negating the need to possess all functions internally. By affording numerous redundant function options through the combat cloud, individual platforms no longer need to leverage as much from their internal attributes, nor do countries and their services need to organize, train and equip to operate "organically" to achieve "self-sufficiency." Additionally, the combat cloud vision reduces the pressure to over-load requirements and allows individual platforms to evolve in a more cost-effective fashion. The result is that individual systems are freer to strive to excel in specific areas. For its part, the combat cloud supplements a broader array of capabilities and ultimately serves as a more effective and efficient means to achieve the intent of "jointness."

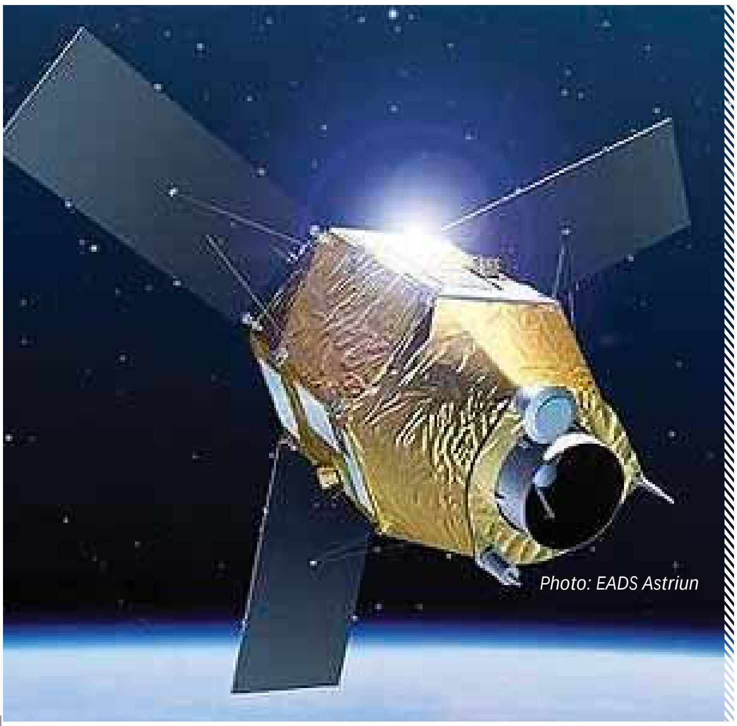


Photo: EADS Astriun

The same holds true for allied interoperability. Partners around the world are modernizing their armed forces with new military capabilities that have the potential to enhance the effectiveness of a combat cloud-enabled force. Some examples of specific systems include F-35, Eurofighter Typhoon, Aegis-equipped ships, P-8, Wedgetail Airborne Early Warning and Control (AEW&C) aircraft and Eurohawk among others. Transforming these individual weapon systems into collaborative elements of an interdependent operational enterprise is what the combat cloud is all about. Whether discussing technical standards, common training standards, or established operational tactics, the potential afforded by individual allied systems will only be realized if they are harnessed in an organized, deliberate fashion.

The physics of future combat platforms will likely not change significantly but how these systems operate within future battle networks must change to realize the potential of 'informationized' warfare. In order for combat forces to freely access and distribute information during combat operations, some existing platforms will need modification but more importantly partner countries and armed services must develop gateways and relevant infrastructure to share information in a ubiquitous and seamless fashion.

This has become the "industry standard" for global civil commerce and it must become the new normal for allied militaries. Becoming a fully 'informationized' force will require defense leaders to recognize that ISR is a combat mission that must be controlled and protected by fielding weapon systems focused on that objective.

Conclusion

In an era of constrained military resources perhaps the best bet on achieving the ability to defeat asymmetric threats and plugging gaps in the allied sensor-shooter network is the notion of actualizing the combat cloud. This approach will not only change the way we define new requirements but, more importantly, the way we think about C2 and operating these systems. This is the essence of the combat cloud – it is not just about the network but about the entire enterprise of sensors, shooters, and connectors all part of a cohesive, coherent whole extending across all operating domains.

The future demands an agile operational framework for the integrated employment of allied military power. The next step is shifting away from a structure of segregated land, air or sea warfare to truly integrated operations, strategically adopting the idea of cross-domain synergy. The complementary versus merely additive employment of capabilities in different domains is such that overall effectiveness is enhanced and vulnerabilities are better compensated. This combined effects approach is about integrating existing and future operations across all the domains with an agile operational framework guided by human understanding. As such, this is more of an intellectual construct with technological infrastructure than the other way around and requires dominance of the electromagnetic spectrum at the appropriate times and places.

The actualization of the combat cloud will not be easy and it is sure to upset many well established ways of operations and culture – but it is inevitable and if we fail to realize such a vision we have too much at risk to let our adversaries do so instead.

Lieutenant General (Ret.) David Deptula is Dean of the Mitchell Institute for Aerospace Studies in Arlington, Virginia, United States, and is a Senior Military Scholar at the U.S. Air Force Academy. He was the principal attack planner for the 1991 Operation Desert Storm air campaign; Commander of no fly-zone operations over Iraq in the late 1990s; Director of the air campaign over Afghanistan in 2001; Twice a joint task force commander; and Air Commander for the 2005 South Asia tsunami relief operations. He is a fighter pilot with more than 3,000 flying hours–400 in combat–including multiple command assignments in the F-15. His last assignment was as the Air Force's first Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR), where he transformed the United States' military ISR and drone enterprises – orchestrating the largest increase in drone operations in U.S. Air Force history. He retired from the U.S. Air Force in 2010 after more than 34 years of distinguished service.

Lieutenant General (Ret.) David Deptula

Photo: General Atomics

Remotely Piloted Aircraft: The Challenges of Force Integration

Dr. Gary Schaub, Jr.
Centre for Military Studies, *University of Copenhagen*

Military Uses of Remotely Piloted Vehicles (RPAs)

In 2002 an American Predator remotely piloted aircraft (RPA) launched a Hellfire air-to-surface missile at a suspected terrorist target for the first time in history. This was an important threshold in the sixty year pursuit of remotely piloted flight. Since then, the success of RPAs – and the attention paid to these new weapons of war – has driven demand and stimulated supply throughout the international system. According to the U.S. General Accountability Office, between 2005 and 2012 the number of state possessors of RPAs "nearly doubled from about 40 to more than 75". As of 2017, ten countries possessed armed RPAs – namely, the UK, US, Saudi Arabia, Israel, China, Pakistan, Iraq, Iran, Nigeria, and Turkey – and of these, only Iran and Saudi Arabia have yet to use those systems in combat.

Technological innovation and operational requirements have produced considerable variation among RPAs including large and small, fixed-wing and rotary-wing variants, a variety of propulsion sources, from battery power or solar power on smaller systems to internal combustion or turbofan engines on larger systems. Some can operate only within line of sight and others beyond line of sight, depending on communications capabilities. The U.S. Air Force distinguishes between small unmanned aerial systems (SUAS) and RPAs as depicted in Table 1 below:

Table 1: Representative Air Force Platforms versus Joint UAS Group Classification

	UAS Groups	Maximum Weight (lbs)	Normal Operating Altitude (ft)	Speed (Kts)	Representative Aircraft
SUAS	Group 1	0-20	< 1,200 AGL	<100	Raven (RQ-11); Wasp
SUAS	Group 2	21-55	< 3,500 AGL	< 250	Scan Eagle
SUAS	Group 3	< 1,320	< FL 180	< 250	Currently No USAF Program of Record for this Category
RPA	Group 4	> 1,320	< FL 180	Any Airspeed	Predator (MQ-1)
RPA	Group 5	> 1,320	> FL 180	Any Airspeeed	Reaper (MQ-9); Global Hawk (RQ-4)

> Stabilization, counter-insurgency, and counter-terrorism have provided the context for the relatively rapid development, acquisition, and employment of RPAs for most Western militaries

Photo: Northrop Grumman

Three factors have shaped the acquisition and integration of RPAs: First, whether they have been developed and manufactured domestically or acquired through international arms sales; Second, whether acquisition satisfies an urgent operational need, and; Third, whether the acquisition is designed to develop long-term airpower capabilities.

Initially, the small number of countries that could develop and produce RPAs generally limited supply and many states compensated by acquiring SUAS to provide a limited range of tactical capabilities. Over the past decade, however, RPA availability has slowly ramped up as new suppliers have entered the market. The U.S. has restricted export of its Predator, Reaper, and Global Hawk RPVs to a limited number of NATO allies such as the United Kingdom, Italy, the Netherlands, Germany, and France and major non-NATO allies, such as the UAE, Japan, Australia, and South Korea. But the U.S. may loosen these restrictions within the context of its October 2016 Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs). French exports of Sagem's Sperwer tactical RPA to NATO allies during the 2000s have been eclipsed by Israel's global export of the Heron, Hermes, and Hunter RPAs starting in the mid-2000s, according to the Stockholm International Peace Research Institute. China entered the global export market in 2014 when it sold five armable RPA to Nigeria and Iraq. As other suppliers enter the market, limited supply of military-grade RPAs will no longer be a primary barrier to acquisition. But acquisition by no means equates to effective employment or integration into a larger military force.

Acquisition Drivers for RPAs - The Canadian Experience

Acquisition of RPA capabilities can be driven by urgent operational requirements realized in conflicts at hand. For the entirety of the modern RPA era, these conflicts have primarily been low intensity expeditionary conflicts taking place in permissive air environments. Stabilization, counter-insurgency, and counter-terrorism have provided the context for the relatively rapid development, acquisition, and employment of

RPAs for most Western militaries. The requirement has been for persistent tactical surveillance of mobile small units and individuals utilizing cover and concealment, particularly in areas populated by civilians. Furthermore, the intelligence yielded by these systems must be distributed in real-time to ground forces that are often in close proximity to, and often engaged with, adversary forces. This is often done via a portable line of sight (LOS) control terminal organic to the ground unit, whether man-portable or mounted on a vehicle. The intelligence, surveillance, target acquisition and reconnaissance (ISTAR) yields could also be sent back to headquarters for further analysis and exploitation. Such intelligence is necessary to find and fix enemy targets, protect friendly forces, and to conduct operations with minimal collateral damage. This latter requirement derives from Western preferences for establishing stable and legitimate governance in its conflicts, as delineated in American and NATO military doctrine.

Within this context most instances of RPA acquisition in the midst of conflict have been directed toward joint operations in support of ground forces. This has had a significant impact on the ability of militaries to integrate and utilize these new capabilities effectively. Canada's experience with RPAs acquired to meet urgent operational needs suggests some of these impacts. Canadian participation in Operation Enduring Freedom provided an impetus for the Army to drive Canadian RPA policy. Canadian forces soon recognized that the hazards of "persistent indirect fire" required beyond the LOS imagery for which the Army lacked appropriate equipment (Little 2008: 50–1). The Army undertook to acquire a tactical RPA system under an expedited process for urgent operational requirements.

The Army opted to purchase the Sagem Sperwer RPA – a French-made tactical RPA system – to provide for the ground commander's ISTAR requirements. The choice was a surprise to senior Air Force officers who believed that the Army would acquire a smaller hand-launched SUAS. The Army chose to locate the RPA in an artillery regiment given their previous experience with target drones. Air Force doubts as to their competence led to five rated pilots and additional technical staff supporting the regiment's RPA unit. A steep learning curve and operational issues encountered in Afghanistan effectively resulted in lackluster performance, the withdrawal of the unit, and the reconsideration of RPA operations by the Canadian military (Kenny 2012: 27; The Field Artillery School 2005: 20).

The result was a UAV Campaign Plan that made the Air Force primarily responsible for the acquisition, employment, and sustainment of RPAs with a take-off weight greater than 84 kilograms, including tactical RPAs such as the Sperwer and any future medium altitude long endurance (MALE) RPAs such as the Predator and high altitude long endurance (HALE) RPAs such as the Global Hawk. Upon returning to Afghanistan, a Canadian Air Force helicopter squadron operated an enlarged fleet of Sperwers supported by the artillery unit that had previously "owned" the airframes. They were replaced by a maritime aircraft squadron when Heron MALE RPAs replaced the Sperwers in 2009. The twenty-five Sperwer aircraft flew 4,270 hours on over 1300 missions and only six crashed during three years of operation, while Herons flew 837 missions during their 30-month deployment and none were lost. Providing the capability in the right organizational framework significantly increased their effectiveness.

The successful deployments did not lead to institutionalization, however. The helicopter and maritime air squadrons returned to their primary missions after Canadian operations in Afghanistan ceased and the Herons, which had been leased, were returned to the manufacturer (Renni 2011). The Canadian Air Force's knowledge, experience, and capability of utilizing RPAs to provide ISTAR to ground forces was discarded in favor of service priorities because it was an "interim capability" explicitly tied to an urgent, and passing, joint operational need. They did not contribute to the service's long term capability plans. Furthermore, Canadian Forces had not yet institutionalized joint targeting and relied upon partners to supply that capability. Overall, Canada lacked a joint reconnaissance-strike battle network to provide an institutional and intellectual home for its RPA capability and no organic community that "owned" the assets or mission. Without these key institutional developments, RPAs were a disposable niche capability whose full potential was never realized.

Acquisition of RPAs can also be driven by long-term capability development. Peacetime investments in systems determined to provide new, improved, and/or additional capabilities are routinely made. Yet new military technology that has the potential to substantially increase capabilities is normally expensive. Significant investment in such capabilities requires the ability to make the case effectively –an easier task if they improve the ability to perform existing core missions in traditional ways. Disruptive innovations often require changes in doctrine, tactics, techniques, procedures, training, and organizational missions and practices. Such innovations are more complex, impinge upon a greater variety of stakeholder equities, and often have a narrow experiential basis to recommend themselves. Military forces have difficulty adopting and integrating disruptive innovations—as again illustrated by the experience of Canada with RPAs.

> Disruptive innovations often require changes in doctrine, tactics, techniques, procedures, training, and organizational missions and practices

Canada's Joint Unmanned Surveillance and Target Acquisition System (JUSTAS) program was established in 2000 with the objective to yield an operational RPA capability by 2009. The program first evaluated a few small systems before being diverted to handling the Army's acquisition of the Sperwer discussed above. The Canadian Air Force bifurcated the JUSTAS program in August 2006 to accommodate the different requirements of expeditionary ground operations and other potential uses of RPAs. The first was to concentrate on MALE RPAs that could be used over land in expeditionary operations in temperate climates and the second would focus on MALE and HALE RPAs suitable to maritime use, with "surveillance in the North" a key mission (March 2007; MacLean 2005: 5).

Canadian Challenges in Harnessing RPAs

Ambitious objectives were set to adopt this "transformational technology" within 18 months. The MALE RPV should stay aloft for more than 24 hours, have a panoply of sensors, potentially carry weapons, and be operated over distances beyond line of sight (BLOS), preferably from Canadian territory (March 2007: 10). BLOS control from Canadian territory would permit "moving the entire mission crew to a fixed ground control station… [and] allow the number of personnel deployed into a theatre of operations to be significantly reduced" as well as enable Canada-based "mission crews to be managed more efficiently between operations at multiple locations" (Jaggi and McCorquodale 2009: 35). Furthermore, as the new concept was implemented, "many of the manned aircraft practices and procedures [would] have to be adapted to fully exploit emerging UAV technology" (Jaggi and McCorquodale 2009: 35). In all, JUSTAS would substantially "change the way the Air Force conducts military flying operations" (Jaggi and McCorquodale 2009: 35). A new Chief of the Air Staff soon realized "that proved a little too complicated, a little too difficult for us to get through the system, so we walked it back a bit" (MacLean 2007: 8).

Such transformation was shelved while the interim solution of the leased Herons provided support for ground forces in Afghanistan. Upon the dismantling of that deployable capability, attention returned to long-term planning via the JUSTAS program. Despite a five year holding pattern, the Air Force remained undecided on what was required. JUSTAS was supposed to "provide the mandatory capabilities for domestic and international operations [to] complement existing reconnaissance, surveillance, and target acquisition capabilities, increase maritime and arctic domain awareness and provide precision force application in support of Land and Special Operations Forces" (Department of National Defence, undated). It was left open as to whether these tasks required one, two, or more systems. Despite the passage of another five years and the acquisition of RPVs by many Canadian allies — including the Netherlands, Italy, Germany, France, and the United Kingdom—Canada is still bereft any specific plan to acquire, let alone integrate, a RPV system. Canada's latest defense strategy, released in June 2017, states that it will "invest in a range of remotely piloted systems, including an armed aerial system capable of conducting surveillance and precision strikes," which it specifies as "medium altitude remotely piloted systems" (Government of Canada 2017: 73, 39). The anticipated timeline is approval of a definition of requirements by 2020, a request for proposals by 2021, contracts to be awarded by 2024, and final delivery between 2026 and 2036 at a cost of $500 million to $1.5 billion (National Defence and the Canadian Armed Forces, 2016). As with many such long-term capabilities that have yet to prove themselves and develop a constituency, RPAs are not a high priority for the Canadian Air Force.

Conclusion

Despite great enthusiasm and expectations that RPAs could provide significant airpower capabilities at relatively low cost, the ability of medium and smaller powers to acquire, integrate, and employ larger and more sophisticated systems has been quite limited. It has been realized, although perhaps not by political leaders, that RPAs have a logistical footprint — including airfields, runways, shelters, armaments, and support networks that are similar to manned aircraft. They also require manning roughly equivalent to that of manned aircraft – although a typical MALE RPA may have a crew of two (one pilot and one sensor operator), over 50 personnel are required to operate four aircraft from one ground control station and many more to process and distribute the sensor data gathered (Royal Air Force, undated). Establishing the institutional infrastructure for a real-time reconnaissance-strike battle network that integrates sensors and shooters, in dispersed manned and unmanned platforms, in national or expeditionary environments, is perhaps the key challenge of integrating RPAs. Indeed, the ability of an air force to do so will be indicative of its ability to transition effectively into a 5th generation force.

Photo: General Atomics

References

Anonymous Royal Canadian Air Force officer. 2014. Personal correspondence. August 6.

Anonymous. 2013. "Canadian Forces UAV Procurement: A DND JUSTAS Project Timeline." *Canadian American Strategic Review*. Available at http://www.casr.ca/id-justas-project-timeline.htm, accessed 11 August 2014.

Anonymous. Undated. "CF Leased UAV—McDonald Dettwiler/IAI Malat CU170- Heron," *Canadian American Strategic Review*. Available at http://www.casr.ca/-101af-cu-170heron-uav.htm, accessed 12 August 2014.

Report on Major Crown/Transformational Projects, available at http://www.forces.gc.ca/en/about-reports-pubs-departmental-performance/-2012 section-iv-status-report-major-crown-transformational-projects.page#JUSTAS, accessed 11 August 2014.

Field Artillery School, The Royal Regiment of Canadian Artillery. 2005. "The Year 2004 in Review," *The Canadian Gunner* 39, pp. 15–14.

Government of Canada. 2017. *Strong. Secure. Engaged. Canada's Defence Policy*. Ottawa: Department of National Defence.

Jaggi, Ulrich and Andrew McCorquodale. 2009. "UAVs: A -40Year Overnight Success," *FrontLine Defence* 1 ,6, pp. 34.

Little, Richard. 2008. "A Short History of Surveillance and Target Acquisition Artillery," *Canadian Army Journal* 3 ,11, pp. 53–43.

Maclean, Chris. 2007. "LGen Angus Watt: Air Force invests in the Future," *FrontLine Defence* 5 ,4, pp. 8–4.

March, William A. 2007. "Learning to Walk?" *FrontLine Defence* 6 ,4, pp. 11–8.

National Defence and the Canadian Armed Forces. 2016. "DAG 2016 Aerospace Systems Services: Joint Unmanned Surveillance and Target Acquisition System." May 26. Available at http://www.forces.gc.ca/en/business-defence-acquisition-guide2016-/aerospace-systems59-.page, accessed 18 June 2017.

Renni, Steve. 2011. "Military to Disband Drone Team after Afghan Mission Ends," *The Globe and Mail.* January 11.

Dr. Gary Schaub is a Senior Researcher at the Centre for Military Studies, Department of Political Science, University of Copenhagen in Denmark and Consultant to Institute for Defense Analyses in Alexandria, Virginia, United States. He previously was Assistant Professor of Strategy at the U.S. Air War College, a Research Fellow at the U.S. Air Force Research Institute, a Visiting Assistant Professor at the U.S. Air Force School of Advanced Air and Space Studies, a Researcher at the Center for International Studies at the University of Pittsburgh, as well as serving as Adjunct Assistant Professor of History at Chatham College in Pittsburgh, United States.

Dr. Gary Schaub

Trends in Ballistic and Cruise Missile Technology and its Impact on Counterforce Planning - A South Korean Perspective

Sung Kurl Kim Ph.D.,
Research Fellow, *Korea Institute for Defense Analyses (KIDA)*

Missile Proliferation around the World

It has been over 25 years since the end of the Cold War but advanced weapons such as ballistic and cruise missiles are continuously building up with the international proliferation of missile technology. Missile systems, used only by Germany during World War II, are now used by dozens of countries. Moreover, due to the constant development of missile technology and test-fire exercises by countries possessing missile systems, ballistic and cruise missile systems are today increasingly more mobile, survivable, reliable, and accurate, and of course can achieve greater ranges.

Among states that possess missile technologies, Russia and China are considered to have particularly advanced capabilities – and both view missiles as symbols of national power. Russia and China are both focusing efforts to enhance missile technologies, particularly in terms of accuracy and flight velocity. Over the years, in fact, numerous types of ballistic and cruise missiles have already achieved dramatic improvements in accuracy. In the past, when missiles offered only low accuracy, some users often found it necessary to install weapons of mass destruction warheads. However, recent technology improvements now allow numerous types of ballistic and cruise missiles to be used effectively with conventional warheads. Moreover, the greater accuracy of missiles also enables precision targeting of hardened targets, such as underground bunkers, which was not possible during the mid-1980s.

Photo: Lockheed Martin

States with advanced missiles have recently also begun working on developing ballistic missile-launched hypersonic glide vehicles (HGVs). HGVs are able to combine the advantages of velocity from ballistic missiles and the accuracy of cruise missiles. As HGVs maneuver at a speed of greater than Mach 5, it is very difficult to defend against them using current missile defense systems. Russia and China are making efforts to develop HGVs to counter existing missile defense – namely, with the YU-71 (also known as Project 4202) in Russia, and the DF-ZF (previously designated as the WU-14) in China.

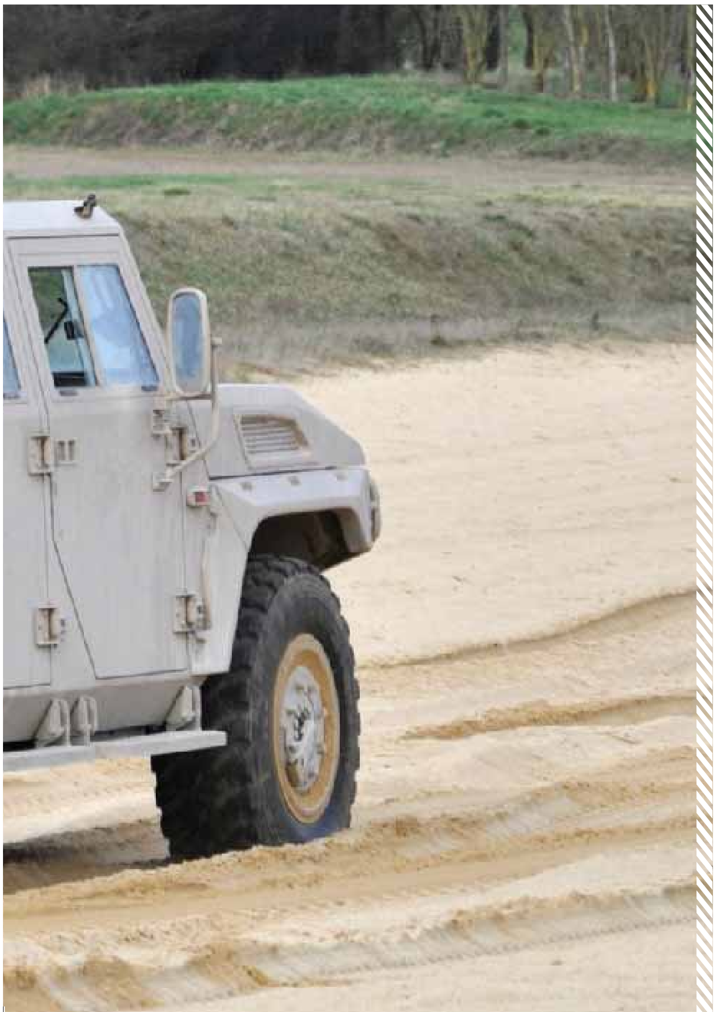
States that have more recently developed missile technologies such as North Korea, Iran, and Syria are however arguably the greater sources of threat to international stability today. North Korea and Iran are both developing intercontinental ballistic missiles (ICBMs) as a way to strategically counter the United States and coerce neighbors with the threat of destructive capabilities. Both Pyongyang and Tehran have launched satellites into orbit with space launch vehicles (SLVs) – and since SLVs and ICBMs use inherently similar technologies, the successful development of ICBMs by these two states is an increasingly likely plausibility. North Korea in particular is now conducting test-fires of its missiles at very short intervals and developing missile technologies in defiance of sanctions imposed by the UN Security Council. Missile test-firing by North Korea is provocative to neighboring states and undermines regional stability. Through recent tests, North Korea has demonstrated intensified efforts to extend the range of its missiles and introduce new and more sophisticated variants than ever before.

Photo: Thales Group

North Korea's Development of Diverse Missiles and Increased Ranges

Kim Jong Un, North Korea's leader, mentioned in his 2017 New Year's Address, "We entered the final stage of preparation for the test launch of intercontinental ballistic missile." In response, U.S. President Donald Trump on January 2, "North Korea just stated that it is in the final stages of developing a nuclear weapon capable of reaching parts of the U.S. ... It won't happen!" However, despite international condemnation of North Korea's destabilizing nuclear and missile proliferation activities, the strategic environment is evolving in unfavorable directions.

On July 4, 2017, Pentagon spokesman Captain Jeff Davis acknowledged that the ballistic missile North Korea test-fired over is "not one we've seen before." He also confirmed the latest ominous sign that the standoff with the reclusive regime over its sanctioned missile and nuclear programs is reaching crisis point. The test-fired North Korean ballistic missile can travel more than 5,500 kilometers, putting Hawaii and Alaska within targeting range. North Korea also seems to be close to developing ICBMs capable of reaching the U.S. mainland.



Recent test-fires have demonstrated the significant success achieved by North Korea in increasing the ranges of its missiles. The development of ICBMs by North Korea has become possible through the development of a new engine and propulsion system. On September 20, 2016, KCNA reported that Kim Jong Un had overseen the testing of a large new rocket engine at the Sohae Satellite Launching Station, claiming the new engine had a thrust of 80 tons – putting it in the range of 160,000 pounds or 80,000 kilograms force. Furthermore, North Korea claims it has acquired re-entry technology which is an important element in developing ICBMs.

However, as North Korea has so far only conducted ground-testing of re-entry vehicles (RVs), many analysts speculate that its trials to date may not have achieved the conditions necessary to demonstrate workable RV technology. It is however plausible that North Korea may have acquired RV technology of a certain level, though it may be incomplete for the time being. As it stands, Pyongyang now possesses short-, medium- and long-range ballistic missiles, largely deployed from mobile launchers although the Pukkuksong missile (also known as KN-11) is a submarine-launched ballistic missile (SLBM). Ballistic missiles launched by North Korea have so far used liquid-fueled propulsion systems but its KN-11 test-fired in August 2016 is believed to have used solid-state fuel technology.

North Korea's tenacious efforts to acquire a diverse collection of missiles has not stopped at ballistic missiles but has extended to developing cruise missile with very high levels of accuracy. During North Korea's April 15 military parade, a mobile-tracked-vehicle was on display that conducted a cruise missile test-fire last June – it was previously test-fired in February 2015 as well. The missile seemed to be lookalike of the Russian 3M24 Uran (SS-N-25 Switchblade) anti-ship missile which is a state-of-the-art anti-ship missile capable of sea-skimming flight.

A Path to Countering Missile Threats

As missile technologies improve, defending missile attacks has become a more difficult and complex task. For instance, with the improving accuracy of missiles, the number of targets also increases and the successful interception of incoming missiles has become more challenging given the large diversification of missile types today. Cruise and ballistic missile users have always retained a set of advantages over those states pursuing missile defense – which is inherently more difficult. Strengthening missile defense must also contend with advancing in a cost-effective manner in order to be a realistic and sustainable measure.

> As interception technology is limited, to deter or disrupt the missile launch itself could be a more effective and desirable

Under such circumstances, planning for missile defense must integrate a number of strategic and technological considerations. As missiles with improved accuracy and strengthened attack operation capabilities can cause tremendous damage it is important that they are intercepted during their flight phase, if not before. Since active defense measures in missile defense and in particular interceptor missiles are extremely costly, they also raise challenges of cost-effectiveness. As interception technology is limited in reality so as far as it is possible preemptive operations to deter or disrupt the missile launch itself could be a more effective and desirable.

The most critical element of missile defense is the ability to achieve threat early warning (TEW), which can come through reinforcing intelligence, surveillance, tracking and reconnaissance (ISTAR) assets. ISTAR assets in missile defense include a network of land-based, airborne, and space-based sensors. Fortunately, advances in ISTAR technologies have made possible the detection, or threat early warning (TEW), of most missiles when they are launched or even the activity preceding launch.

During Operation Desert Strom in 1991, synthetic aperture radar (SAR) – a key ISTAR capability – could not image moving targets and hence there was limited effectiveness of space-based sensors in hunting mobile missiles. Over the past two decades however ISTAR technologies have achieved progress with, for example, data-processing techniques that enable SAR to detect moving targets as well as accurately determine their speed and direction of travel. SAR-equipped satellites are now able to find mobile targets and have the potential to transform counter-TEL operations. For example, a SAR-equipped satellite can now generate up to twelve 150 km by 150 km frames in a single pass before passing over the horizon – enough to image all roads in North Korea more than once and key sections multiple times.

Today, manned aircrafts with SAR and Ground Moving Target Indicator (GMTI) radars have the capability to create high-resolution images of stationary targets or track a large number of moving vehicles. However, most manned surveillance aircraft must operate from "standoff" distances to reduce their vulnerability to air defenses and generally also have more limited endurance for continuous flying operations. Moving forwards, efforts need to focus around developing measures to utilize unmanned aerial systems (UAS) for ISAR missions, which are increasingly designed to be stealthy and penetrate adversary airspace.

In states with large territories, ISTAR missions using UAS may prove more difficult but for states with smaller territories it could be possible to find ways to reconnoiter from outside the territory of threatening states. According to recent research, for example, the RQ-4 Global Hawk UAS in four continuous orbits 80 km outside North Korean territory was able to observe and identify targets on 54 percent of North Korea's roads – and when four RQ-4 Global Hawk UAS were used the coverage increased to 84 percent. If target reconnaissance zones are have flat topographies – such as deserts or plains – the use of manned aircrafts or stealthy UAS do not have much difference however when the area of interest is mountainous – like in North Korea – where roads are hidden behind terrain, then stealthy UAS can execute ISTAR missions more effectively. Although mobile transporter-erector-launcher (TEL) can change location before launch, it is stored most of the time in underground tunnel networks.


Photo: Lockheed Martin

To launch a missile, the doors of underground tunnels need to be opened or the TEL must be moved – if UAS can monitor underground tunnel networks and facilities continuously, signals can be detected prior to impending missile launches. Moreover, if UAS could be armed with attack weapons they could prove crucial in further deterring missile launches.

If TEW can be effectively achieved then it is possible to counter missile launches with interceptor missiles more accurately and cost-effectively. For neutralizing incoming missiles attention may also shift to field artillery which can enable precision attack operations unlike before. Newly developed field artillery systems have successfully demonstrated enhanced capability when employed together with improved artillery munitions technology. For example, 155mm field guns can achieve ranges of nearly 180 kilometers today. Alternatively, large-caliber multiple rocket launchers have much improved accuracy given their ability to change the trajectories of fired artillery shells during the terminal phase. Large-caliber multiple rocket launcher are becoming a useful means for missile defense not only because it is difficult to differentiate artillery and missiles, but also because the cost of multiple rocket launchers is comparatively much lower than missiles. Together with high-technology systems such as Patriot and THAAD an effective balance set of capabilities to shoot down incoming missiles can create an effective missile defense shield.

Yet the challenge of missile defense crucially requires international cooperation if objectives are to be successfully and sustainably achieved. Missiles are offensive weapons which have asymmetric effects due to their capacity to be employed for surprise attacks and because of their relatively low costs. An effective response to missile threats, which effectively threaten much wider regional security, is actively pursuing international cooperation program with partners to both share required tasks and work together collaboratively.

International cooperation at the basic level includes building a common awareness of missile threats and the sharing information between partners on missile developments from threatening states, if there are no political barriers in doing so. Building on such basic exchanges, international cooperation can then be deepened to the point at which sharing of intelligence-sharing can occur, with reconnaissance and ISTAR information, for example, as well as sharing means of interception, and conducting joint exercises for missile defense. The U.S.-Israeli military exercise named "Juniper Cobra" is an example of how practicing together allows partners to work through key interoperability challenges in responding to a potential missile crisis. The U.S. Air Forces Central Command (AFCENT) also maintains a series of regular exchanges Gulf Cooperation Council (GCC) air defense officers. These mechanisms provide opportunities for exchanges to build and enhance shared situational awareness of missile threats in the region as well create new possibilities for future missile defense planning and operational cooperation.

Conclusion

Missile technology is advancing rapidly today to overcome difficulties typically encountered during early stages of missile development. Some rogue states around the world are increasing the level and complexity of missile threats and endangering regional stability through the rapid and dangerous development of missile technology. On the other hand, technology to support missile defense has not yet caught up and in fact the gap between missile technology and missile defense technology is increasing. Within such a backdrop, missile defense planning must move on from the limited approach of neutralizing launched missiles in-flight with interceptors and consider a multi-faceted approach that is built on effective international cooperation with partners. Such an approach that successfully offsets the asymmetry and strategic advantages enabled by missile systems can moderate the momentum of missile development and provide stronger rationale to these states for reverting to political negotiations.

Sung Kurl Kim joined the Korea Institute for Defense Analyses (KIDA) as Researcher in 2007. His current focus is on projects dealing with missiles, missile defenses, and North Korea's proliferation of missile. Kim is a former reporter for the Hankyoreh daily newspaper during which he covered the Ministry of National Defense for 13 years. He holds a bachelor's and a master's degree in political science, and a doctorate in Korean missile defense. Sung was a Visiting Fellow at the The Center for Strategic and International Studies (CSIS) in Washington, D.C., United States in 1999, and the Institute for National Strategic Studies (INSS) at the National Defense University, Washington, D.C., United States, in 2006. He is the author of numerous publications on foreign policy and on defense strategy.

Sung Kurl Kim

Photo: Saab

The Future of Integrated Air Power and Missile Defense in the Arabian Gulf

Thomas Karako and Wes Rumbaugh
Senior Fellow and Research Assistant, *Center for Strategic and International Studies (CSIS)*

Today's Threat Environment

The ongoing Yemen war provides insights into the future character of conflict. Over the last two years, rebel Houthi militias have fired dozens of missiles at targets ranging from power stations to air bases to civilian areas. In response, Saudi Arabia and the United Arab Emirates have employed Patriot missile defenses to intercept numerous threat missiles and defend important assets. The complexity of even this seemingly lower-tier fight like this nevertheless serves to illustrate the demand for networked integration, coalition interoperability, and multi-domain awareness. The Yemeni Missile War serves as a kind of harbinger of the complex and growing air and missile threats for the Middle East and beyond.

More missiles fired in anger have been intercepted in the Yemeni hostilities than during any other conflict in history (Figure 1). The Yemeni Missile War has not been confined merely to ballistic missiles, and neither is the complex and growing air and missile threat set. This includes air breathing threats like anti-ship cruise missiles and unmanned aerial vehicles (UAVs) for both strike and reconnaissance missions. The combination of these capabilities presents a wide spectrum of challenges for the United States and its partners, including with respect to Iran.

Although the Joint Comprehensive Plan of Action (JCPOA) may forestall Iranian nuclear development in the near term, the absence of restrictions on missile testing and development leave a significant strategic issue unresolved. Growing regional interest in missile defenses suggests that Gulf nations view them as a hedge against both conventional missile attack and nuclear breakout. A joint statement by GCC foreign ministers and the United States after the JCPOA pointedly welcomed the progress on ballistic missile defense and arms transfers as previously agreed at the 2015 Camp David Summit.

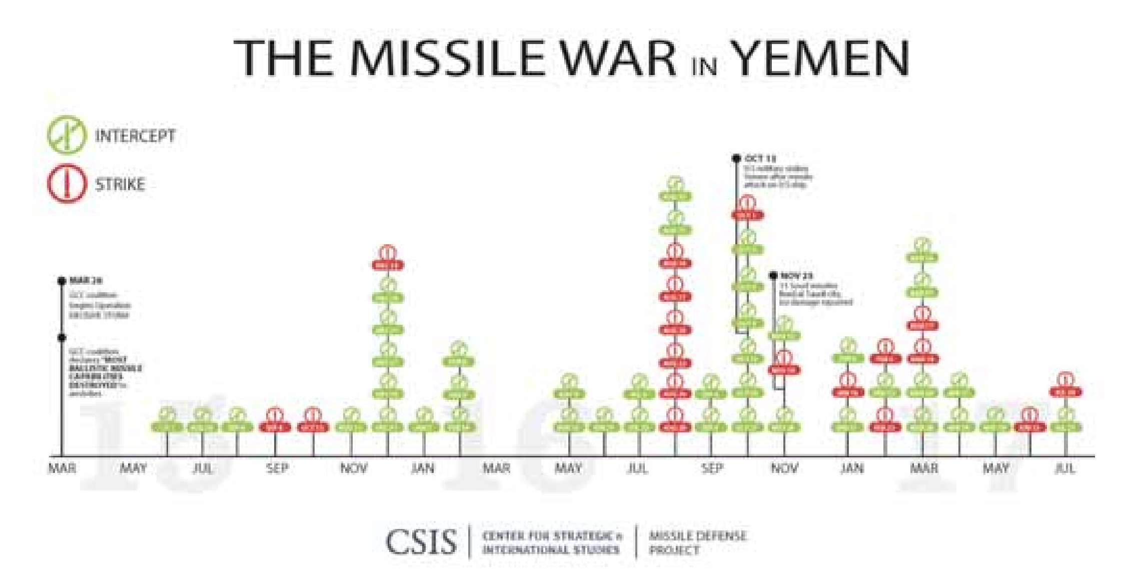


Figure 1

This past year, several Gulf nations announced plans to make further missile defense purchases –with billions of dollars in investments likely. Increased missile defense capacity is important, but will be insufficient if it not part of a larger and more comprehensive strategy. The United States laid out detailed plans with the European Phased Adaptive Approach (EPAA), but no comparable plan with milestones has yet been articulated for missile defense in the Gulf. The several EPAA milestones included the deployment of Aegis ships at Rota, Spain and later the construction of Aegis Ashore sites in Romania and Poland, progress towards which includes the broadening defense capability for NATO territory in Europe. Some levels of coordination are certainly still possible but with increased testing and the operational use of the Zolfaghar missile in Syria, the time may be ripe to develop such a path. Greater coordination and cooperation can result in a more effective defense for all – the sharing of early warning data, enhanced interoperability between partner nations, and movement towards a common air picture can go a long way towards making regional air and missile defenses more effective.

Active air and missile defenses alone, however, will be insufficient. The United States and its Gulf partners cannot afford to simply sit and play catch. A more comprehensive approach is necessary; one which effectively integrates defenses with strike forces. Such an approach would leverage the significant air power deployed by Gulf nations and demonstrated during the counter-ISIS and Yemeni campaigns, will be important to attrite adversary missile forces in future conflicts. Such a posture would constitute a move to defeat missile attacks, rather than simply defend against them.

Regional Missile Threats

Iran possesses the largest and most diverse missile arsenal in the region, with several families of missiles that include short-range artillery and rockets, as well as longer range ballistic and cruise

Figure 2

missiles (Figure 2). Iran's missile development program includes both liquid-fuel missiles and an expanding arsenal of solid-fuel missiles, which can be fired more rapidly and are more mobile, complicating the task of destroying them before launch. These developments are informed by Tehran's experience during the Iran-Iraq War in the 1980s, which saw large numbers of ballistic missiles fired during the War of the Cities. This combined with a deteriorating air force, have caused Iran to develop significant numbers of missiles, and work to upgrade the accuracy of its arsenal.

Some commentators have argued that the JCPOA removes the strategic threat posed by Iran, but serious concerns remain about Iranian conventional missile capabilities. Part of this challenge arises from the sheer number of missiles Tehran might fire, but recent advances in missile accuracy are of even greater concern.

Several recent developments confirm that missiles represent a key component of Iran's military strategy. The use of several ballistic missiles to strike an ISIS compound in Deir ez-Zor in June 2017, for instance, demonstrated Iran's willingness to employ such systems in combat. Tehran initially slowed its missile testing during JCPOA negotiations, but launch activity has since increased (Figure 3). Iran is also placing increased emphasis on solid-fuel ballistic missiles, which are more mobile and capable of prompt launch.

Figure 3

Tehran has also tested anti-ship cruise missiles against a mock aircraft carrier, sending a clear message about its intent in a potential conflict with the United States. In February 2017, Iran tested the Soumar, a cruise missile that could potentially reach into southern Europe. In the Syrian conflict, Iran has used UAVs both to support airstrikes with Sadid missiles and also for surveillance and to support targeting for strikes from other platforms.

Iran Regional Strategy

Iran's missile force supports its regional military posture in several ways. First, Tehran uses missiles to support a version of an anti-access/area denial strategy (A2/AD) to restrict regional freedom of action for U.S. and GCC militaries. By threatening key nodes like military bases or points of debarkation, Iran hopes to be able to deter adversaries by raising the costs of any conflict. Even without the ability to strike discrete targets accurately, Iran's missile arsenal allows it to raise the cost of intervention to oppose its actions by threatening softer targets like cities and economic infrastructure. In the Yemeni conflict, missiles have targeted both military and economic sites, as well as population centers.

To further support its A2/AD approach, Iran has invested in improved air defenses, including the purchase of Russia's S-300, delivered in October 2016. Combined with other indigenous air defenses, the S-300 complicates the ability of Gulf nations to exploit their relative advantage with fixed wing aircraft. Improved air defenses may also point towards the need for greater standoff capability and low-observable strike aircraft.

Secondly, Iran uses its missile arsenal to support proxies, as evidenced by the strikes on ISIS to assist Bashar Al Assad in Syria. This sort of informal extended deterrence allows Iran to expand its influence in the region, causing significant concern to its GCC neighbors. Iran also supports its proxies by means of direct transfer of missiles, as evidenced by the continuing conflict in Yemen as well as with Hamas and Hezbollah. While the Houthi insurgents captured many of the former Yemeni government's ballistic missiles, the continued use of missiles suggests some sort of Iranian support to refresh their stocks. The United States and GCC members have intercepted weapons shipments into Yemen, including coastal defense cruise missiles. Similar missiles significantly damaged an Emirati ship and also fired on the USS Mason (DDG-87) in October 2016. The supposedly Yemeni-produced "Burkan" missile bears a strong similarity to Iran's Shahab family of missiles.

Strategic Value of Missile Defenses

The tactical and strategic value of missile defenses can also be seen in the ongoing conflict in Yemen. Saudi and UAE Patriot forces have intercepted a significant number of missiles targeting air bases and civilian areas fired by the Houthi rebels. The aforementioned USS Mason incident illustrates how active missile defenses help control crisis escalation. Should the anti-ship missiles have struck the U.S. vessel, a significantly greater American retaliation would likely have been necessary. Because of the combination of kinetic and non-kinetic defenses aboard the ship, however, the United States had the luxury of responding in a manner and level of its choosing, in this case with targeted strikes on radar stations guiding the missiles. The high intercept rate of Patriots in the Yemen conflict has no doubt dramatically limited damage to military and civilian targets.

> The high intercept rate of **Patriots in the Yemen conflict** has limited damage to military and civilian targets

Missile defenses also bolster deterrence by ensuring freedom of action and offsetting adversaries' anti-access and area-denial capabilities. Protecting critical military facilities and civilian centers supports the ability to respond effectively to aggressive actions, and thereby strengthens deterrence. In the case of the Middle East, missile defenses to protect GCC military forces would reduce Tehran's incentive to take early preemptive action in a crisis.

In light of growing threats, the United States and GCC members have purchased and deployed significant missile defense capacity. The United States has forward-based Patriot batteries in the UAE, Bahrain, Qatar, and Kuwait. Saudi Arabia, UAE, Kuwait, and Qatar have also purchased Patriot for themselves. In 2012, the UAE became the first foreign nation to purchase the THAAD system, with the first battery becoming operational in 2016, and a second battery on the way. In May 2017, a proposed U.S.-Saudi arms deal announced the potential purchase of seven THAAD batteries. In addition to capacity, there is also an important need to improve the capability of interceptors. Cooperative development, like the current U.S.-Japan program to build the Standard Missile-3 Block IIA missile, could help offset research and development costs helping to deliver advanced capabilities more quickly. In 2016, Under Secretary of Defense Brian McKeon testified that the UAE had offered to subsidize development of an extended-range THAAD interceptor. Should a similar co-financing arrangement be pursued in the future for THAAD or Patriot modernization, the additional capabilities would have applications both in the Middle East and elsewhere, including the Asia-Pacific and Europe.

GCC investment in missile defense interceptors has been strong, but missile defenses would further benefit from increased sensor coverage and the creation of a single, integrated air picture. Missile defenses cannot hit what they cannot see, and a greater density of sensors would contribute to resilience in the face of an attack on the currently limited number of radar sites. Elevated sensors may also be necessary to counter non-ballistic threats. Iranian investments in land attack cruise missiles suggest the need for sensors to detect and track low-flying threats.

Interoperability and Network Centrism

The United States and the GCC have on multiple occasions reaffirmed their intent to work toward "a Gulf-wide, interoperable missile defense architecture." So far, however, such coordination and interoperability remain all too aspirational. To the extent that networking and integration also lag, it hinders the full effectiveness of investments made to date.

Photo: Lockheed Martin

Part of the problem is a lack of integration between the systems themselves. A priority for the United States is to improve the interoperability of its own systems as a means to simplify integration of partner capacity. To this end, the U.S. Army is currently developing the Integrated Air and Missile Defense Battle Command System (IBCS). When fielded, IBCS will improve the efficiency of missile defenses by allowing better coordination between firing units and defense against a broader spectrum of threats, including UAVs and cruise missiles.

The next step could be to improve interoperability between states. Coordination and a common air picture lengthens decision times, improves situational awareness, reduces interceptor wastage, and also helps avoid potential fratricide. Such coordination and cooperation could be especially beneficial considering the short distances that Iranian missiles must travel to reach targets in GCC states. This too involves challenges, as nations must be convinced that the benefits of sharing data outweigh the costs. The military utility, however, seems clear.

Due to geography, the early warning radar that Qatar is considering purchasing would provide a significant advantage to early warning of missile strikes, as well as to developing a common air picture. Numerous questions have yet to be resolved between Qatar and other GCC members, but the potential military utility of such cooperation seems clear.

Integrating Gulf Air Power

Another key area ripe for Gulf cooperation is air power, which can contribute to both the development of a more common air picture and serve to strike adversary missiles before launch. Multiple sites already work on integrating United States and coalition air assets, including the Combined Air Operations Center at Al Udeid Air Base in Qatar and the Gulf Air Warfare Center hosted by the UAE. These centers offer a basis

Photo: Boeing

for creating a single, integrated air picture, which could significantly improve coordinated air operations between partners in the Gulf. Further efforts could work to integrate the various F-15, F-16, F/A-18, Mirage, and Typhoon fighters deployed by Gulf states, as well as the airborne early warning and control aircraft deployed by Saudi Arabia and the UAE.

Continued development of air power platforms also present an opportunity to improve the sensor picture for not only air operations, but also integrated air and missile defense. Integration of data from sensors on UAVs currently deployed by the United States and Gulf partners could help fill gaps in persistent overhead coverage, improving the detection of cruise missiles. Future purchases of fifth generation aircraft like the F-35 could also support such a network-centric approach to air operations. The design of the F-35 as a sort of 'flying combat system,' capable of integrating sensor information from multiple platforms and serving as a battle management hub, could contribute significantly to combined air operations.

Integration would also better support the combination of air and missile defenses with offensive strike operations to destroy missiles or other threats left of launch, before they can be fired. Gulf states can leverage their significant air power used in the counter-ISIS campaign to this end, and could diversify their strike platforms by purchasing upgraded cruise missiles. Strike capability is a key component of countering Iran, but expectation control is also important about the ability to destroy missiles prior to launch. In early 2015, Saudi Arabia believed that air strikes in Yemen reduced much of the missile forces on the ground, but those predictions proved too sanguine. Additional missiles have since been brought to bear, and with numerous missiles raining down on coalition partners in the three years since. In air power, the benefits of coordination are similar to those in air and missile defense.

The integration of both strike and defense forces to defeating threats both left and right of launch with a variety of effectors are necessary to progress toward more interoperable, and potentially even integrated air and missile defense forces within individual state militaries and across the region. The ability to coordinate strikes effectively between states would reduce wastage of munitions and increase their effectiveness by offsetting air defenses. Coordination of air power assets can also reduce the risk of fratricide among partner aircraft in a cluttered and complex operating environment. The ability to plan and conduct air operations cooperatively among the United States and its partners in the Gulf would also be a strong deterrent signal to Iran.

Conclusion

The growing supply of air and missile threats and the demand for means to counter them represents a trend that will not abate any time soon. In the face of these threats, the United States and its Gulf partners will need to together develop a comprehensive approach to defeat these threats and negate the coercive potential from common adversaries.

Thomas Karako is a Senior Fellow with the International Security Program and Director, Missile Defense Project, at the Center for Strategic and International Studies (CSIS) in Washington, D.C., United States. His research focuses on national security, U.S. nuclear forces, missile defense, and public law. He is also an Assistant Professor of Political Science and Director of the Center for the Study of American Democracy at Kenyon College, Ohio, United States. During 2010-2011 he was an American Political Science Association Congressional Fellow, during which he worked with the professional staff of the House Armed Services Committee on U.S. strategic forces policy, nonproliferation, and NATO.

Thomas Karako

Wes Rumbaugh is a research assistant in the International Security Program at CSIS. Previously, he was director of advocacy and a Van Cleave fellow at the Missile Defense Advocacy Alliance. He holds a BS in Political Science from Missouri State University.

Wes Rumbaugh

Airpower in Counter-Terrorist Operations: Balancing Objectives and Risks

Adam R. Grissom Ph.D. and Karl P. Mueller Ph.D.
Senior Political Scientists, *The RAND Corporation*

Harnessing Air Power in Counter-Terrorist Operations

Violent non-state actors, including terrorist networks, pose a real if limited threat to the citizens of virtually every state in the international system. The operations of these networks, individually and collectively, are also corrosive to the stability and functioning of the international system as a whole. It is therefore natural that the more capable and responsible states in the system have attempted to employ their instruments of power, including military power, to mitigate both the proximate and the broader challenges posed by terrorist networks. Given the growing number and potency of these networks since the 1990s, "counter-terrorist (CT) campaigns" have not surprisingly become a hallmark of contemporary international politics.

In recent decades most, if not all, the air forces represented at the 8th Dubai International Air Chiefs Conference have been involved in efforts to disrupt, deny, deter, and/or ultimately defeat terrorist networks. While the coalition operations in Iraq and Afghanistan have garnered much of the public attention, efforts to bring military power to bear against terrorist networks have of course extended well beyond those countries and this region. Today there are more CT campaigns underway in more places, conducted by more powers and coalitions against more adversaries, than ever before.

In recent years a growing number of these efforts have taken the form we call "limited-liability, limited-objective campaigns" in which major powers cooperate with local forces (official or irregular) to disrupt and exert pressure on non-state adversary networks located in areas that are chronically under-governed or otherwise uncongenial to more comprehensive stability operations. These campaigns are not necessarily aimed at transforming the socio-political conditions that make an area conducive to adversary networks and therefore they offer slim prospects for decisive victory. The de facto objective is often limited to mitigating the threat posed by the adversary network or networks. The assets and resources devoted to these campaigns by major powers are likewise limited to relatively small numbers of special forces and air assets with a "small footprint" located outside the area of direct operations or perhaps a small number of locations within the operational area.

The strategic basis of limited-liability, limited-objective campaigns is therefore quite narrow. The primary aim of the major power – which faces a threat from the enemy that may be significant

Photo: WAM

but is far from existential – is simply to disrupt the operational capability of an adversary network for some period of time. The assets, resources, and even political capital expended are minimized along with risks to metropolitan forces. The partnership with local forces may be temporary and transactional. The essential calculus is that the limited strategic benefit of temporarily disrupting the adversary network exceeds the limited strategic costs and risks of the campaign. By our count more than two dozen such campaigns are currently underway around the world.

Lessons Learned for Air Power in Counter-Terrorist Operations

The most striking characteristic of limited-objective, limited-liability campaigns is their fundamental reliance on airpower. In these circumstances, airborne assets are vital to every phase of what has come to be known as the "find, fix, and finish" cycle of targeting nodes in terrorist networks. Airborne intelligence, surveillance, and reconnaissance (ISR) assets are essential to illuminating terrorist network topography and to finding key individuals and groups in the network and characterizing them as targets in the campaign. Airborne ISR is likewise vital to fixing key objectives so action can be taken against them. And of course in many cases air assets are the preferred means of delivering effects to the objective, whether in the form of munitions or strike teams.

What is often less recognized is the equally essential role that airpower plays at the operational level of these campaigns. Coalition forces generally move to and from the operational theater by air, they are repositioned within the theater by air, and as noted above they often conduct operations unilaterally or with partner nation forces primarily from the air. Coalition forces – both ground and air units – are typically based at airfields, they are typically commanded from facilities at airfields, they survive on logistics delivered mostly over aerial lines of communication, and they rely on weather forecasting, communications networks, and a myriad of other aerospace capabilities with an airfield at the epicenter. In many ways, with little public fanfare, the expeditionary airfield has emerged as the sine qua non of the modern CT campaign.

All of this implicitly underscores an existential strategic reliance on airpower that is even more easily taken for granted. With their reliance on persistent overhead ISR coverage, tactical air mobility, and aerial firepower to protect assets on the ground, contemporary CT campaigns can scarcely be contemplated under any conditions except air supremacy. The freedom to exploit the aerospace domain at will is the central military advantage of modern states over adversary networks. CT campaigns are naturally, if often only semi-consciously, built around this advantage. Airpower – both ISR and precision strike – also underpins CT campaigns as one of the deterrent factors contributing to contemporary terrorist networks, unlike their predecessors, being predominantly non-state entities rather than state-sponsored ones.

The development of air-centric limited-liability, limited-objective counter-terrorist campaigns amounts, in our view, to a significant military innovation. The political leaders of major powers have framed a challenging strategic problem for their armed forces: mitigating the threat posed by terrorist networks where conditions are such that standard assistance or resource-intensive conventional stability operations are unlikely to yield a positive strategic return on investment. The armed forces of the major powers have responded by devising air-centric campaigns that attempt to strike a favorable balance between operational cost and benefit.

Many lessons have certainly been learned in this process of innovation, as suggested by the striking similarities among CT campaigns conducted by different (even antagonistic) major powers. At the tactical level, the primary lesson is undoubtedly that finding and fixing are enormously more important and more difficult than finishing. The tempo, precision, and scale of effects achieved against such enemies are all primarily determined by the degree to which the adversary network can be characterized and its key nodes fixed in time and space. Human intelligence obviously plays a tremendous role in that process. For external powers, however, airborne ISR is the name of the game. Yet for many air forces, ISR perplexingly remains a "low density, high demand" capability category (a matter of concern not limited to CT operations).

> **At the tactical level, finding and fixing are enormously** more important and more **difficult than finishing**

At the operational level the most important lesson is arguably the importance of fusing operations and intelligence effectively. Every adversary network is different, and friendly action against a competent network will trigger response and adaptation. The art and science of orchestrating an effective campaign of action against a clandestine human network is the height of CT campaigning. Doing it well, of course, requires overcoming traditional organizational boundaries, not only between services but among military and non-military agencies, and multiple participating nations.

What is even more striking than the lessons learned about air-centric CT campaigns in recent years, however, are the questions that remain unresolved. Leaving aside the various tactical and technical controversies, there are myriad fundamental operational and strategic issues that have not received the detailed analytical examination that one might expect. These include the relative effectiveness of decapitation and attrition targeting campaigns, the effects of concentrating on particular alternative target sets within them, and the nature of the relationship between number of assets committed to a campaign and its effects on the adversary network (which may be linear or non-linear, or perhaps both depending on conditions). Even basic issues such as whether the unintended (or for that matter the intended) casualties caused by CT targeting campaigns mean that they "create more enemies than they remove from the battlefield" have been subjected to little systematic analysis, though scant evidence has not discouraged pundits and partisans from making confident assertions about the answer.

Conclusion

In sum, we might draw an analogy between the state of the art of CT campaigning today and the state of operational airpower innovation in the period immediately after the 1991 Gulf War. A great deal of tactical and operational experience has been accrued by a variety of major powers. Yet, unlike the 1990s when the Gulf War Air Power Survey and numerous other studies sought to analyze the operational effectiveness and lessons of that campaign, many of the fundamental questions that will guide the evolution of the air-centric CT capability to maturity still remain under-examined.

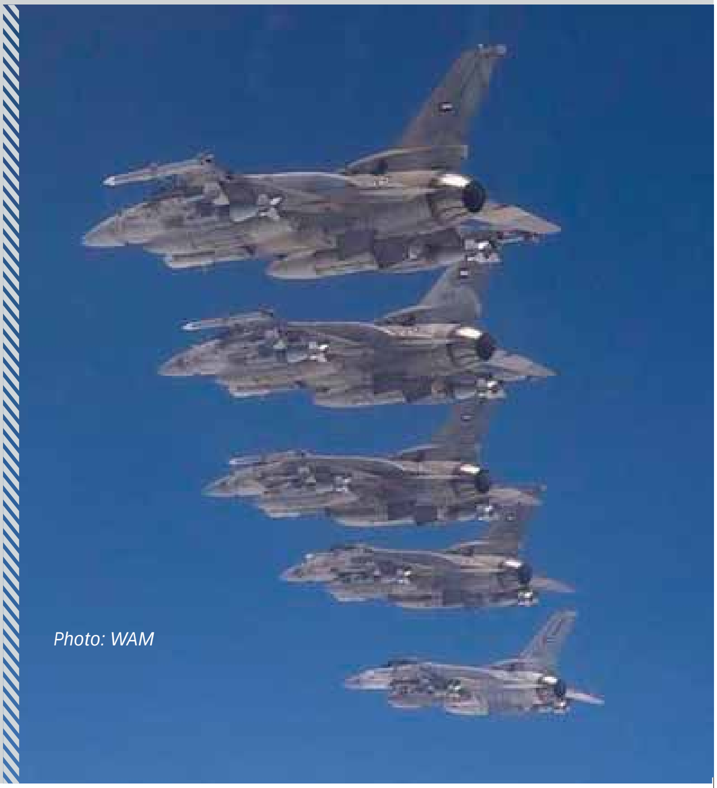


Photo: WAM

This is important to air forces because the primary challenge in further developing CT capabilities is conceptual rather than material in character. While some sophisticated systems have been employed in CT campaigns, the essential aerial tools are not technically complex compared to those required for fighting advanced state adversaries. What is extraordinarily complex and challenging, however, is the orchestration of those tools with all the other elements of national power to achieve the desired disruptive or deterrent effects on an adversary network. It is this intellectual problem that poses the greatest limitation today for the development of CT capabilities in powers great and small.

References

1- Definitions of "terrorist" vary, and often exclude groups that operate within war zones or that attack military instead of civilian targets. This discussion applies the term broadly to include a variety of non-state networks that resemble terrorist organizations in structure and function.

Adam Grissom is a Senior Political Scientist at the RAND Corporation in Santa Monica, California, United States. He leads a group that conducts special mission analysis for the U.S. Department of Defense and allied ministries of defense. Adam's external academic work focuses on innovation in military organizations. He lectures on the subject and serves as a reviewer for The Journal of Security Studies, International Security, the European Journal of International Studies, and Studies in Conflict and Terrorism. Prior to joining RAND in 2000, Adam was a civil servant in the Office of the Secretary of Defense. He holds a Ph.D. in War Studies from King's College London, UK, a master's degree in Public Policy from Harvard University, United States, and a B.A. in Political Science from Augustana College, Rock Island, Illinois, United States.

Adam Grissom

Karl Mueller is a Senior Political Scientist at the RAND Corporation in Santa Monica, California, United States, and teaches at Johns Hopkins University, Baltimore, Maryland, United States, and at Georgetown University's School of Foreign Service in Washington, D.C., United States. He writes and lectures on a wide variety of national security subjects, including deterrence and coercion, airpower theory and history, crisis stability, economic sanctions, nuclear proliferation, space weaponization, and legal and moral issues in the use of military power. Dr. Mueller's most recent RAND publication is Precision and Purpose: Airpower in the Libyan Civil War and his current projects focus on NATO defense strategies for the Baltic States and designing wargames for the analysis of potential future conflicts. Prior to joining RAND in 2001, he served as a professor of Comparative Military Studies at the U.S. Air Force's School of Advanced Air and Space Studies (SAASS), at Maxwell Air Force Base, Alabama, United States. He holds a Ph.D. in Politics from Princeton University, New Jersey, United States, and a B.A. in Political Science for the University of Chicago in Illinois, United States.

Karl Mueller

Exploiting Network-Centric Operations (NCO) for Information Superiority

Sabahat Khan
Senior Analyst, *Institute for Near East & Gulf Military Analysis*

Air Power beyond the Air Force

Just over a century ago, the leading military powers of Europe were the first to realize the utility of aviation in warfare – first for reconnaissance purposes and then as platforms that could deliver bombs. As aerial capabilities of militaries rapidly grew in subsequent years to exploit the benefits they provided, the 'Air Force' was established as an independent service like the Army and Navy – first by the British and followed by countless other powers. From the First World War onwards, air power came to figure pivotally in military competition and warfare.

Ever since, nations have become accustomed to the Air Force playing an indispensable role in defense – more than ever before, militaries are unable to achieve mission objectives in high-stakes or complex operational scenarios when air superiority does not exist or when air power cannot support operations in the land or naval domains. That reality applies to warfighting of course but extends to almost the full spectrum of military operations other than war (MOOTW), from humanitarian to peace-keeping operations.

A new strategic transition is however underway in defense – the air domain is effectively expanding into space/near space and, along with the land and sea domains, a powerful cyber domain has emerged. These domains, as militaries are learning today, are complexly integrated and cross-cutting in nature. As a result, militaries have begun turning attention to building cyber power and integrating these into a more effective Joint capability. Such an approach promises the best optimized integration and application of capability to achieve the right effect at the right time in a whole-of-force sense.

The growing prioritization towards Joint capability may well refocus military activity back towards greater Army 'ownership'. Separately, armies and navies have continued to develop advanced aerial capabilities of their own, often using the same platforms used by air forces – reconfigured to their unique operational environments and user needs. As these trends continue, future air power is unlikely to continue remaining a largely Air Force-focused remit as it has been in recent decades and will instead be a capability that is increasingly cascaded across different branches of the military in new and novel ways. The evolution of remotely piloted vehicles (RPAs) that carry sensors to provision intelligence, surveillance and reconnaissance (ISR), carry weapons, and even support transport operations will undoubtedly have a strategic role to play with how militaries at large, not just the Air Force, approach future air power in a holistic sense.

Looking further out, the long-term future for the Air Force may appear as uncertain as it is exciting. The world's leading air forces are already embarking on the introduction of highly intelligent 'fifth generation' fighter aircraft that will be stealthy, highly networked with sensors, effectors and other platforms, and rely heavily on automation. Some experts have suggested – with good reason – that emerging 'fifth generation' fighter aircraft now being inducted into service by NATO nations could well be their last major development of manned fighter aircraft because the future will belong almost entirely to RPAs.

The Primacy of Information Superiority

Air superiority has rightly come to be regarded as essential to winning wars: In the words of Field Marshal Bernard L. Montgomery, "If we lose the war in the air, we lose the war and we lose it quickly." Since the Nazi attack on Poland in 1939, in fact, no country has won a war when their adversary exercised air superiority – no major offensive has succeeded and no defense has sustained against an opponent that controlled the air domain. We are yet to see a state lose a war while it has maintained air superiority. Yet, emerging trends would suggest that air superiority will not remain the single most decisive factor in military conflict or competition much longer.

> Air superiority has rightly come to be regarded as essential to winning wars

It is likely that space/near-space superiority or a combination of space and cyber superiority will become more crucial elements in determining the outcome of future conflicts rather than air superiority as we view it today. One justification for such an argument would be that without a combination space/near space and cyber superiority it would not realistically be possible to achieve air superiority in as little as decade from now. Command, control, communications, computers, intelligence, surveillance, tracking and reconnaissance (C4ISTAR) and battle management (BM) are already becoming heavily reliant on space-based systems. As that development consolidates further, the weaponization of not only the cyber domain that underpins connectivity to remote systems but space/near space itself will become inevitable. It is unclear if the Air Force will ultimately lead defense into space, or if an altogether new service will need to be established for what is likely to be the ultimate frontier in military competition.

Ultimately however it will be information superiority that will become the single most decisive determinant of future conflicts and military competition. Information superiority could be understood to logically represent the greatest aggregated sum of military capability in a future where limiting factors such as range,

Photo: U.S. Air Force

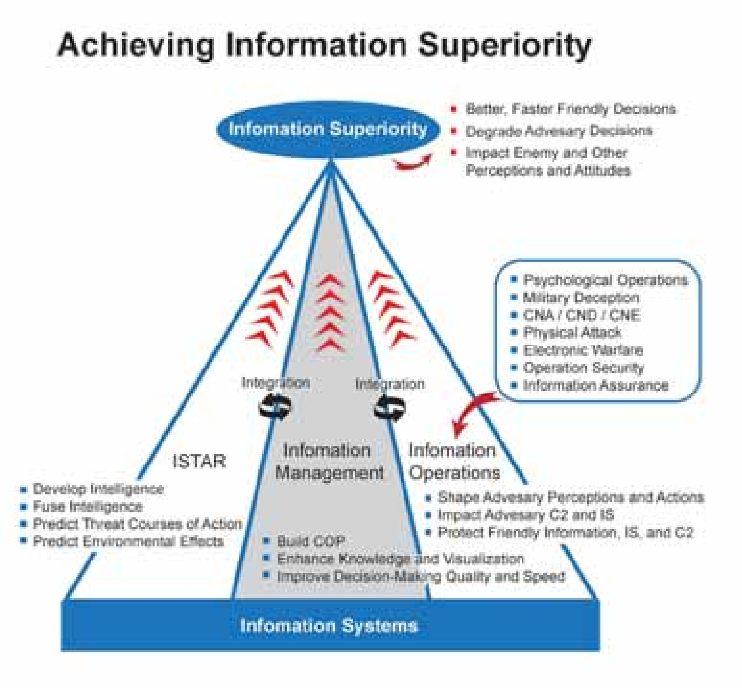
precision, and destructive power for offensive weapons will effectively become irrelevant. Multi-domain battlespace dominance will be determined by information superiority that enables forces to meet mission objectives in highly compressed decision-time cycles. Successful execution of planning, operations and battle management to deliver the right effects at the right time will hinge on information superiority rather than the sophistication of systems making up advanced military platforms – in the air or otherwise.

With ongoing efforts to transform towards network-centric operations (NCO) the pursuit of information superiority is already underway. NCO is a concept of operations (CONOPS) that promises a sum greater than its parts by integrating multiple layers of networks together to provide greatly expanded situational awareness that is shared at an enterprise-level as close to real-time as possible. As a CONOPS, NCO attempts to provide the 'enabling' framework with which to pursue the effects-based operational approach (EBOA). EBOA is, in concise terms, the ability 'to see first, understand first, act fist, and finish decisively' and NCO enables this by providing a network-wide capability to securely deliver the right information to the right personnel in the right way, with the right meaning and at the right time – all the time.

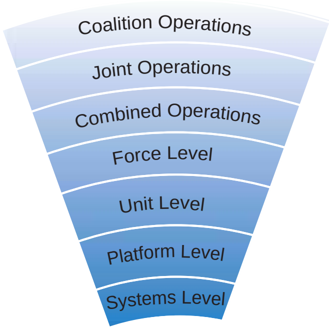
Challenges with Technology and Human Factors in Exploitation

Implementing NCO requires capability-based planning (CBP) approaches that can translate strategic requirements into an operational architecture for resourcing missions or courses of action (COA) effectively. As CBP moves beyond platform-centrism to meeting capability development more holistically and strategically, translating user needs into system requirements accurately and then procuring the equipment that provides the right functionality, performance and interoperability is crucial.

Equipment is however but one element of CBP and capability management needs to be synchronized other key elements such as concepts and doctrine, organization, personnel, training, logistics, information, and infrastructure – all the while considering and working to accommodate and exploit potential capability contributions that can be made by allies or coalition partners for specific scenarios. At both layers, the design, operation and sustainment of connecting networks is critical for



Levels of Interoperability



Dominating the Information Environment

Inputs	Outputs
Seamless Architecture and Systems Integration	Enhanced Command and Control
Responsive information Collection, Processing, and Dissemination	Fused, All-Source Intelligence
Prioritized Requirements and Assigned Responsibilities	Precise Situational Understanding
Information Operations	Degraded Adversary C2

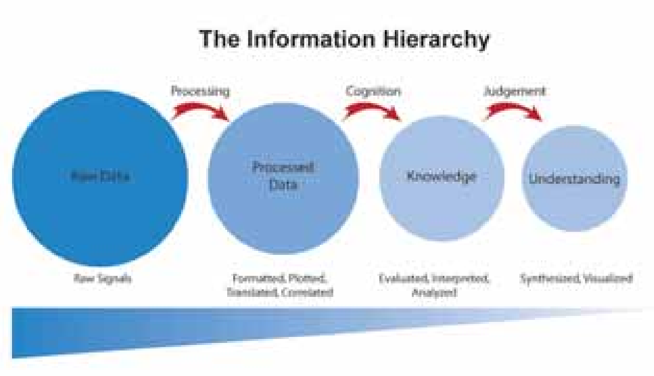
the engineering of capabilities for frontline forces. As such, exploiting advances in NCO or effectively harnessing fifth-generation capabilities is a highly strategic and nuanced effort – going beyond simply acquiring the latest systems and widgets or narrowly focusing on system-to-system interoperability considerations in equipment plans. One of defense's most glaring truisms today is that man-made technologies have advanced at faster pace than the ability of its user to exploit their true potential. Successful transformation towards NCO and the pursuit of information superiority will actually rely more heavily on human factors than on making technology smaller, faster, lighter, stronger, more efficient, and, more 'interoperable'.

Process automation and artificial intelligence promise a level of reliability, accuracy, efficiency, and output that humans cannot match. It may be many years before humans allow C2 to become automated at the strategic level, if ever. However technology is already not only helping the Air Force and counterparts in other services make tactical and operational decisions but increasingly making those decisions for them. Mission failure or measures of performance that do not meet anticipated results in operations can almost always be assigned to human error at the command, operator, or logistics and support levels. Moreover, in almost all cases, information systems could have either prevented those errors from occurring in the first place or have provided forewarning about failure to mitigate and manage the consequences better. Fortunately, the right tools are already available – the challenge today is how well they can be adapted, and how well those that will use those tools can adapt their own approaches to exploit such aids.

Information?

Militaries have, broadly speaking, performed poorly with managing information systems – from not collecting information at all to not collecting information accurately or collecting information that was not required, recording information in the wrong formats or standards, not storing information in the right place, not sharing information where it should have been or not sharing information at the right time, and failing to interpret information as it was intended to be are common problems. As it stands, information in defense at large exists with large gaps, tucked away in stovepipes, has low reliability and still remains tightly controlled by its 'owners' – all at a cost to operational performance and force readiness objectives.

A more recent emerging trend for militaries has been to collect as much information as possible –compounding the problem of poorly managed information assets even further. Typically, militaries have found that their capacity to exploit collected information (when it is actually usable) has not kept pace with their capacity to collect it. Intelligence gathered from RPAs within the space of a few hours, for example, can easily take hundreds of hours to analyze. Yet, militaries remain hungrier than ever for more and new types of information. The acquisition of land-based, space-based, airborne and system-embedded sensors to provide ISTAR continues unabatedly without focusing or investing sufficiently on how to 'understand' instead of only 'seeing' or taking pictures of what is seen.

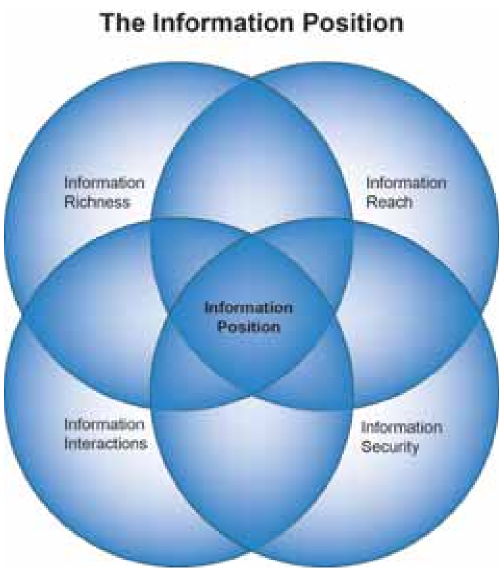


Militaries also lag behind the curve with ensuring situational understanding is shared with the 'many' rather than 'few' – and to do so quickly enough – as a result of a combination of technical but also institutional and cultural barriers. Even today, different services of the same armed forces are reluctant to exchange information with peers and counterparts – and even less so with other national agencies related to national security. Information-sharing internationally is yet even more limited – the reigning approach being that the less information that is shared the better, even with allies. Connecting sensors seamlessly into an enterprise-wide network is arguably the easy part of transforming to NCO in the wider scheme of things because it is largely an engineering task – the biggest challenge to surmount it cultural.

There are indeed good reasons for controlling the type, extent, and frequency of information-sharing –national security, freedom of action, and operational security, for example. There are however better ways to manage the misuse or potential risks of information-sharing than policies that effectively block it from occurring in the first place between services, with 'other' agencies, or allied counterparts. The potential benefits of information-sharing for furthering the security of allies, for example, and receiving in kind, must lead to better rebalancing institutional policies and cultural approaches towards information-sharing.

The costs of poorly managed information systems are hardest felt on the frontline where operational readiness suffers because the right equipment was not delivered at the right place at the right time, for example. Alternatively, good information exploited with intelligent simulation and modeling software can provide critical support to optimize decision-making and operational planning as well as enabling operations to be rehearsed or training activities to be quality enhanced. At best, militaries remain able to utilize such benefits only in pockets and only temporally rather than in a strategic or institutional sense.

Defense has much to learn from the commercial world where, for instance, automotive manufacturers are able to assemble a car within hours in one of several thousand configurations with a combination of 'postponement' and 'just in time' approaches. Automotive manufacturers have been able to achieve exemplary levels of operational performance by removing waste and streamlining processes heavily aided by information systems such as enterprise resource planning (ERP) systems and intelligent business analytics software that together can provide enterprise-level situational understanding – even stretching to multiple echelons of their supply network. Finding the same unity of effort in defense remains more aspirational than a reality even today despite a reprioritization on Joint capability packages.



Conclusion

ERP and advanced analytics software can deliver results only as well as their operators and users can exploit them. Man-machine teaming will remain critical for many years yet and exert a decisive impact on information superiority but technological innovation in, for example, health monitoring systems, quantum computing, and additive manufacture (AM) will radically redefine the man-machine balance in decision-making. Health monitoring systems scaled across entire force structures will transform approaches to logistics and support services together with AM in delivering frontline readiness. Quantum computing will combine with today's nascent data-mining technologies to provide unprecedented computing power for the rapid processing and exploitation or mass volumes of information.

New 'clouds' will emerge to 'push' tailored services and applications to users, advances in network connectivity, bandwidth, speed and spectrum management will transform how the Air Force and military counterparts at large operate. As lessons are learned to harness automation more widely into operational processes it will become possible to largely operate at computing speed. It is at this point that the benefits of whole-of-force network-centrism for enabling EBOA can be truly realized. Until then, it is difficult to genuinely advance the complex effort of achieving information superiority strategically and achieving the output NCO intends to serve.

Information recording, processing, de-confliction, unification, fusion, and dissemination challenges remain a long way from being strategically resolved. Connecting sensors seamlessly into an enterprise-wide network is arguably the easy part of transforming to NCO in the wider scheme of things because it is largely an engineering task. The cultural change required at the human level to lead the transformation of managing, using, and protecting information systems may take a generation for some militaries – less for others. Those militaries and air forces that can effectively make that cultural transformation will set themselves up as best as they can for future.

Sabahat Khan is a Senior Analyst at the Institute for Near East and Gulf Military Analysis (INEGMA) based in Dubai, UAE. His previous research has focused on a range of subjects, including air and missile defense, air power, information operations, maritime security, asymmetric threats and future threat landscapes. His current research focus relates to capability management, engineering support services, and future technologies. Sabahat regularly attends track-two seminars and conferences around the world as a subject matter expert and sometimes features as a commentator with BBC, The National, The Arab Weekly, and Wall Street Journal, among others. Sabahat is a graduate of Cranfield University, King's College London, Royal Holloway University of London, and City University Hong Kong. He is also a PMI-certified Project Management Professional (PMP) and also a Lean Six Sigma Green Belt.

Sabahat Khan

The Future of the 'Air Force' – An Integrated Part of a Broader Defense and Security Eco-System

Stephan De Spiegeleire
Principal Scientist, *The Hague Centre for Strategic Studies*

Introduction - Who Air Forces Are

Discussions about the future of our Air Forces tend to assume that they will look quite similar to today's Air Forces. Most of us expect them to be executing very similar tasks with a capability bundle that is likely to be technologically enhanced but will in essence still remain based on a combination of (preferably manned) steel platforms armed with industrial-kinetic firepower. The purpose of this essay is to question these pervasive assumptions and to sketch an alternative view of future Air Forces that would still aim to achieve similar ends as today but would do so in very different ways and with totally novel means. .

Air Forces are often seen as the 'youngest' service within our Armed Forces, having been 'born' out of our Land Forces sometime around the beginning of the 20th century. This claim reflects an industrial-age view of Armed Forces, in which 'Air Forces' are seen as a child of the industrial age, as it was only then that man reliably mastered the vertical dimension. The famous Wright brothers sold their first real military airplane ('the Flyer') to the US Army in 1909. This means that 'modern' Air Forces have existed in their more 'modern' incarnation for only just a little over 100 years. If we consider the vertiginous changes that are taking place around us in this very day and age, in which more change has taken place in the past few years than in the entire human history, is it really still prudent to assume that Armed Forces in general - and Air Forces in particular - will continue to look the way they have for only the past century?

Air Forces have since their modern origins actively pursued and exploited the physical high ground. The emergence of the vertical dimension - first air and then increasingly also space - has provided Armed Forces with a unique vantage point from which to materialize security effects across the entire battle space. There can be little doubt that this dimension will continue to offer unique leverage over the human terrain where conflicts have traditionally erupted. We can look forward to and have to be prepared for the new waves of innovation that are knocking at our doors in the third and fourth dimensions. Many of these might prove transformational in their own right. But we also see a number of more transformational new 'domains' opening up around us that may require Armed Forces and Air Forces to start thinking differently about who they are.

Beyond then 'Air Force'

Evolving from an embryonic air element within a land component in the early 20th century, airmen and women have jumped on the emergence of this 'new' vertical 'high ground' to exercise 'power' from it. We now see a new and at least equally strategic 'high ground' emerging. Our organizations have, for the time being, christened this the 'cyber' dimension. Just like the 'vertical' dimension was split off from the 'land' dimension in the past, and then bifurcated into an endo-atmospheric third and extra-atmospheric fourth dimension, in the coming decades this 'cyber' dimension may very well also spawn a multitude of different 'domains', which we may not even be able to name yet.

Photo: UAE Embassy, Wasington, D.C.

> In the coming decades this 'cyber' dimension may very well also spawn a multitude of different 'domains'

But the essence of this new 'cluster' of domains is likely to evolve around information and knowledge. This will open up a uniquely 'powerful' high ground that defence and security professionals will be determined to bend to their strategic advantage. Rather than starting a turf-war about who should 'own' these new dimensions, the exponential changes we see around us require us to take few steps back from our usual parochial perspectives and to look from that perspective at the substantive challenges and opportunities we see in front of us and how we can effectively tackle them.

From 'By Ourselves' to 'Through the Ecosystem'

In many discussions, airmen and -women use 'we' in at least 3 different senses: 'we' as members of the Air Force ('we-narrow'); 'we' as members of the Armed Forces ('we-broad'), and 'we' as members of a broader defence and security ecosystem ('we-ecosystem'). The 'logic' in our current thinking now typically runs from left (narrow) to right (ecosystem). We submit that our thinking may have to start running from right to left. Most of our planning and operational efforts are currently focused on 'us' ourselves. 'We' try to get money and political clout for 'ourselves' as militaries, as services. 'We' invest these resources in capabilities for 'ourselves'. 'We' then use these capabilities when 'we' are asked to intervene in conflict situations, typically with other 'we's' - our Allies - that are very much like us.

One of the major changes we anticipate in an 'exponentially' changing world is that this more narrowly defined 'we' will no longer be fit for purpose. We therefore may want to take a very close (and critical and creative) look at whether we may not be better advised to see and position ourselves as the catalysts of a much broader defence and security ecosystem that can provide better value-for-money and more sustainable solutions to some of the complex regional and global security challenges and opportunities that confront of us.

All security challenges we know can best be qualified as complex in nature. They are the – often emergent – result of the dynamic interactions of many interdependent actors and factors. It therefore also stands to reason that the solutions to these complex challenges are also likely to be to be the – again 'emergent' – result of the dynamic interactions of many interdependent actors. We as Air Force or as Armed Forces are but one small actor in a much broader defence and security ecosystem - an ecosystem that we feel has barely been explored, let alone exploited. Maintaining the high ground will also mean taking this broader ecosystem much more seriously than we have so far.

We submit that as military planners and executors, we possess some fairly unique attributes that may put us in a unique position to monitor the 'health' of the ecosystem and to 'nudge' it in the right direction when we observe some particularly dangerous or promising trends. This is not merely an abstract concept. We observe all around ourselves very real yet radically new forms of collaborative purposive action that seem remarkably efficient. Our use of the term 'ecosystem' derives as much from these new forms as it does from the 'ecosystems' we know from nature.

The open source software community, for instance, keeps producing amazing pieces of software (and in quite a few areas even out-competing cutting-edge traditional firms) in a predominantly decentralized and distributed collaborative way, based on entirely new incentive structures and business models and with radically new support systems – typically evolving in vibrant ecosystems that contain both users and developers. In the mobile telephony software realm, companies like Apple and Google have designed 'platforms' (IOS and Android) that have triggered ecosystems in which app developers produce their own software – typically without direct Apple or Google involvement but still to their mutual benefit. In this way these companies coalesce ecosystems of actual or potential stakeholders whom they would never have been able to reach in the traditional way.

Might similar efforts also bear fruit in the defence and security realm? Could we envisage our Defence and Security Organizations (DSOs) establishing analogous 'platforms' on which various third parties may start designing new security solutions? Many of these actors may not even realize they are security stakeholders – like the app developers in our countries but also all over the world who may dream up novel ways of using the avalanche of big (open) data to find creative new solutions to security problems; like the various social networks around the world who are increasingly wielding real 'power' with security effects that they are only dimly aware of; like the farmers in fragile states who can now use their mobile phones to get information on which crops to sow and how to get (micro-)funding for buying the seeds, etc. Have we put enough thought into how we might be able piggy-back on – or even stimulate – some of these efforts in ways that might achieve some of our desired security effects better than we could possibly on our own?

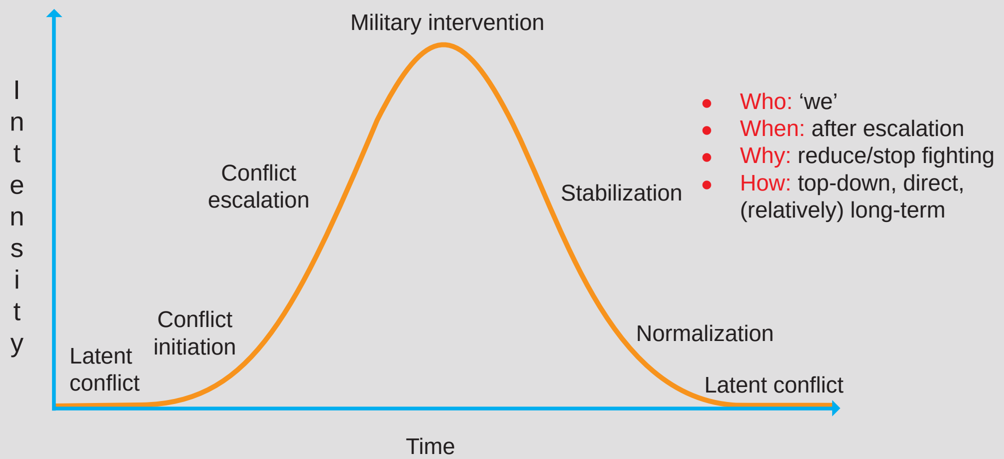
DSOs rarely do things on their own – even today. We work with other DSOs, with international organizations, with other government agencies both in our own and in partner countries, with private companies both inside and outside of the defence industry, with NGOs, with various local communities, etc. But our current 'partner' portfolio tends to be mostly skewed towards heavier, more formalized and bureaucratic forms of cooperation preferably with like-sized, likeminded and 'near-by' organizations that are within our circle of trust. There is still great value to be gained in these forms of cooperation. But how do we gauge, for instance. the return on our investment (in pure 'defence and security' terms) of the (significant) efforts we now put in pursuing synergies with other Armed Forces vs our (now extremely) limited efforts to reach out to organizations like Google, Facebook, IBM or the Gates Foundation? Beyond these well-known ecosystem partners, however, there is a much broader playing field out there that we have barely scratched the surface of and where we might be able to incentivize new forms of cooperation that may prove to deliver exceptional value for money.

What Air Forces Do

Armed Forces currently mostly see themselves – and are seen by others – as 'operators' and war fighters. Air Forces see themselves as the air-borne contributors to that fight. The focus in this paradigm is on 'the enemy' and his order of battle; and the main aim is to defeat them - preferably resoundingly. It has been widely understood (for a very long time - witness the Thucydides trap), that this approach tends to trigger particularly pernicious security dilemmas. Preparing for war typically means that one's opponent(s) will follow suit, and the resulting escalatory spiral may ultimately make all actors worse off. In most of our defense planning efforts, we conveniently ignore that aspect of our efforts.

There is, however, another way to interpret what 'Armed Forces' do. In this paradigm, Armed Forces are there to help provide sustainable defense and security solutions for the societies they protect. That overall task surely includes the need to 'defend' those societies from armed ill-meaning third parties. But it also includes an equally 'real' task to identify or help stimulate security opportunities that might be able to achieve the very same defence and security effects – maybe even in more sustainable and cost-effective ways. Let us take a closer look at two characteristics of how we define our roles today and how these roles are perceived by society.

Our entire way of thinking about defence and security revolves around what some have called the conflict 'hump' (see Figure 1). Our intelligence services and public debates track various locations across the globe where we suspect our interests and/or values might be in jeopardy. 'The military'



equips and trains itself to be able to intervene wherever and whenever tensions have spiraled so out of control in those locations that military means, both kinetic and non-kinetic, are required to defend oneself or to restore stability.

There are, unfortunately, few reasons to expect the need for these conflict-centric tasks to disappear. Our Armed Forces have to stand prepared to continue to provide the necessary conflict response options whenever they are called upon by their political leaders to do so. But there may be better opportunities - also in terms of value for money - to achieve the security effects that we now obtain by intervening massively later in the conflict hump, through more intelligent (and different) interventions at a much earlier stage. Also today, our Armed Forces are already engaged in a variety of ‘conflict prevention' operations, but it is highly doubtful that our current balance of investment between response and prevention efforts delivers optimal performance.

From military operations-centric to a better balance across all echelons

The military as we know it – a separate ‘corps' within the state, entrusted with the planning and execution of military operations under the strategic guidance and political leadership of the top civilian leadership - actually only originated in the 19th century. Prior to this period, ‘sovereigns' (emperors, kings, princes, etc.) essentially incarnated both ‘strategy’ and ‘tactics’. These very same sovereigns would often also lead their troops into battle (which tended to be smaller in size and scope than in the industrial age) and key tactical decisions. We merely point out that the alignment of purposive actions across these two key ‘echelons' was greatly facilitated by the fact that it was embodied in one single ‘full-echelon (strategic-tactical)' commander.

With the advent of the industrial age, new physical as well as social technologies so tremendously expanded the size and scope of military operations that a new echelon emerged that was soon referred to as ‘operational'. It proved no longer possible for a single individual leader or commander to muster the span of control that was required to effectively ‘command and control' the entire effort. From that point onwards the ‘strategic level' of defence and security became separated from the newly emerged ‘operational level'. The former was initially still entrusted to a fairly sovereign echelon but the operational decision-making was relegated to the military corps.

Delving into the complex dynamics of civil-military relationship throughout the industrial age would take us beyond the scope of this essay but we do want to emphasize that divorcing the ‘strategic' from the ‘operational' layer is becoming increasingly unsustainable and even counterproductive. The trend towards more ‘comprehensive', ‘whole-of-government', or even ‘whole-of-society' efforts clearly illustrates this. Today, most stakeholders - and nobody more than us - recognize that there are no exclusively military-operational solutions to any of the security challenges that we are facing. When it comes to operational planning, we have now developed (mainly within NATO, but also in the EU) a protocol that - in our estimation – increasingly does justice to the multiple courses of action that are available to operational commanders and enables us to weigh the pros and cons of these options. This too remains very much 'work in progress'. But at least the protocol allows for a pre-bureaucratic, pre-political, pre-ideological exploration of the theoretical solution space and the development of an actual 'operational plan'. In our assessment, we sorely miss an analogous (and preliminary) protocol at the strategic level.

We have been successful in many, perhaps even most of the tactical and operational engagements that we have fought over the past decades. And yet we did not succeed in obtaining the strategic-level effects we all set out to achieve in many of the theatres we deployed to, from Northern Africa to Afghanistan. We would like to see a broader strategic discussion about available options for better preparing strategic decisions and for then aligning these strategic objectives more organically with activities across these different echelons in today´s much more complex security environment. We now do 'our' thing in theatre. Development workers also do theirs, as do diplomats, Non-governmental organizations (NGOs) and Inter-Governmental Organizations (IGOs). We have all learned to deconflict, and, on rare occasions, to even truly cooperate with each other in-theatre.

We are starting to learn to do the same in our respective capitals with our public and private partners there. But we think there are still many more steps to be made before we can start reaping the benefits of genuine ecosystem-wide (self-) synchronization across various ecosystem partners and across various echelons. Right now, our Air Forces are the 'firefighters' that are called upon to try to put out the fires once they cross a certain critical threshold. But from this 'operational' – in our case 'vertical' – vantage point, we also see various 'strategic' options that we as defence and security professionals could bring to the table to prevent these fires from igniting and/or to ensure that subsequent 'firefighting' efforts prove sustainable. Should we think more about how our Air Forces might be useful not only in the operational but also in the strategic realm.

From Industrial-Kinetic to Post-Industrial (and Non-Kinetic)

Armed Forces have always reflected the era in which they exist. In the Stone Age, we primarily used what little we could find in our immediate surroundings to enhance our own human physical strength and intelligence in pursuing and obtaining defence and security effects. As mankind evolved through the Bronze Age, the Iron Age etc., all the way through the Industrial Age, the development of our militaries evolved in tandem. Europe was the first to 'jump' on the new advantages that the industrial age opened up for the military. Initially, it outclassed most other parts of the world through its competitive approach to defence planning which constantly experimented with teasing new defence and security capabilities out of emerging physical or social technologies. This competition, however, also led to two devastatingly (Euro-) fratricidal world wars that ceded dominance in defence first to the duumvirate of the Soviet Union and the United States. In recent years, we see the tectonic plates of geodefence-dynamics shift again. Most of us still seem to look at these dynamics through industrial-age glasses, One might wonder whether those are still sufficient.

> The essence of our current Armed Forces and our Air Forces in particular very much **reflects the industrial age**

When most of us today think about the concept of 'Armed Force' or 'Air Force,' we conjure up highly hierarchically organized mobile formations of uniformed soldiers equipped with a wide range of physical technologies, based mostly on steel, engines and firepower, employed by national political leaders to advance or defend national goals. While this particular image is by now deeply ingrained in our consciousness, 'Armed Forces' have not always looked like this.

Before the nation-state became the primary actor in the international system (traced back to the Treaties of Westphalia of 1649), 'Armed Force' was exercised by a far more heterogeneous set of actors than just the nation-states (tribes, religious or ethnic groupings, etc.). And prior to the industrial revolution, the physical manifestation of this force looked quite different from what we observe today – not only in terms of physical weapons technologies, but also in terms of the accompanying 'social technologies', including organizational principles, doctrines, regulations etc.

We have to acknowledge that the two key defining features of our current image of Armed Forces, i.e. their state-centered and industrial essence, are under increasing pressure. Both may very well stay with us for some time to come, but we can already detect the patchy outlines of a different era with a much more heterogeneous cast of actors and with mostly new post-industrial physical and socio-technical features (arms, doctrines, organizational structures, etc.). If we assume that humans will continue to avail themselves of whatever they find and can create to attempt to impose their will (in our opinion one of the very few safe assumptions in defence planning), we have to be willing to accept that post-industrial capability packages may look as different from industrial ones as Paleo- or Neolithic warriors from Bronze-age ones; or as armies of medieval knights from the current industrial ones that we are so familiar with.

From 'Punctual' to 'Sustainable' - Where May Armed Forces (/Air Forces) Go?

We are resolute in our determination to remove our industrial age blinders as we go look for and experiment with post-industrial capability

> The Armed Forces, i.e. their state-centered and industrial essence, are under increasing pressure

Photo: U.S. Department of Defense

elements across the security chain. We recognize that, in line with the other 'thinking blocks', this shift requires a broader discussion. Within the Armed Forces. Within our civil services. Within our political systems. Our national societies. Our various alliances. This may very well be one of the key challenges of our time – how we can move to more sustainable stabilization efforts in regions that are afflicted with the multiple pathologies that lead to conflict. Sustainability is creeping to the forefront of strategic thinking in the private sector and many parts of the public sector. In those areas where sustainability is becoming a central theme – as in sustainable energy, sustainable agriculture, sustainable mobility, sustainable architecture, etc. – it is leading to genuinely new ways of thinking and acting. There is, to this day, no real 'defence and security' equivalent. We feel there ought to be.

We find ourselves on the eve of a very different era. Some call it the post-industrial age. It is a somewhat infelicitous term, since the term only designates the old age and does not yet specify the essence of this new age. The most influential driver of this new world, this new society, is likely to be the exponential technological development witnessed in all areas of expertise. Exponential technology development will significantly impact all forms and ways of life, with software playing an ever-increasing role.

We are now increasingly seeing atoms being trumped by bits all around us. We may even call the new era the "Algorithmic era", in which algorithms may very well pack a much more powerful punch ('force') than any airborne military platforms we currently have. This revolution will not only disrupt the way we live our daily lives as individuals (our education, our health care systems, our mobility, our jobs, etc.). It will prompt new forms of society, economy, and polity - including 'Armed Forces'.

Many of us marvel at the technological miracles we see all around us - also in the military world. But in in many ways we still very much live in the 'dark ages'. Our knowledge about ourselves, our brains, our societies, about conflict itself (what triggers it - at an individual or societal level; what are the (de-) escalatory dynamics, etc.) remains disappointingly crude and limited. We are, however, starting to see glimpses of light on the horizon. Major efforts like the human or material genome project are not only giving us our first micro-views of the basic building blocks of ourselves and the physical world around us; but they also opening up new ways for us to start tinkering with these building blocks (see gene-editing techniques like CRISPR-CAS9; or nano-manufacturing).

The proliferation of sensors, effectors and the (increasingly AI-based) algorithms that can link these two together may trigger entirely different forms of 'network-centric' purposive actions – including in the defense and security realm. Key nodes in these networks may be much less the industrial-age platforms we now buy and operate, and much more the individual humans and the societies in which they live.

> Superior situational awareness and understanding of various inter-human dynamics may allow us to move up in the security chain, with the ultimate goal of **preventing conflict (escalation)**

Of making sure that potential triggers of conflict are identified much sooner in their development and defused more effectively at lower cost in a much earlier stage. Could such a more (increasingly artificially) intelligent approach to conflict prevention or resolution become the real new 'High Ground'?

Just as our societies and polities allowed our Armed Forces to capture the industrial-age high ground (in first the third, and then subsequently the fourth dimensions), can we imagine a similar (r)evolution for this new ‘High Ground', thereby morphing their roles from the current-day (industrial-age) warfighters, to tomorrow’s strategic public custodians of a much broader defense and security ecosystem?

Conclusion

The revolution in politics, conflict, warfare and Armed Force that started in 17th century Westphalia was anything but the end of history. Most of the social technologies humans invented in that period (the nation-states; the factory; the modern company; the school district and its schools; the government; the Ministry of Defense; our Armed Forces in their current incarnation, etc. etc.) find themselves under increasing pressure. Do we find ourselves on the eve of an algorithmic revolution that may once again disruptively change all of these social technologies? Only the future will tell. But the present demands that all defense and security professionals start thinking more creatively about who they are, what they do and how they do it.

Dr. Stephan De Spiegeleire is Principal Scientist at the Hague Centre for Strategic Studies (HCSS) in the Netherlands. He was a defense and security analyst at the RAND Corporation in Santa Monica, California, United States, for nearly 10 years in between which he had a 3-year stint at the German Institute for International and Security Affairs (SWP) in Berlin, Germany, and the European Union’s Institute for Security Studies in Paris, France. Since 2004, Stephan has worked at HCSS and The Netherlands Organization (TNO) as well as teaching at Webster University from Missouri, United States, and military academies around the world. Stephan’s main research focus is on security foresight, risk assessment, capability-based planning, performance management, human-centered defense design, and innovation. Stephan’s recent books include Artificial Intelligence and the Future of Defense (2017), The Rise of Populist Sovereignism (2017), Volatility and Friction in the Age of Disintermediation (2017), Better Together. Towards a Defense and Security Ecosystem (2016); Individual Empowerment, Societal Resilience and the Armed Forces (2016), and Designing Future Stabilization Efforts (2014).

Dr. Stephan De Spiegeleire

Photo: Al Jundi Journal

INEGMA

Institute for Near East and Gulf Military Analysis

Disclaimer: The views and opinions expressed in this publication are solely those of the authors and do not necessarily reflect the official policy or position of any agency or any government. Examples of analysis performed within this article are only examples and based only on limited and open source information. Assumptions made within the analysis are not reflective of the position of any government entity or to the organizations with the authors are employed or associated.

Printed in the United Arab Emirates